30 de septiembre de 2021

Análisis de los Eventos de Pérdida de Datos en el 2021 de la Ciudad de Dallas - Informe inicial

Identificación de los tipos de datos perdidos y las posibles causas de los eventos de pérdida de datos en la Ciudad de Dallas en el 2021

Idioma predominante:
En caso de discrepancia entre la versión original en inglés de este informe y la traducción al español, prevalece la versión en inglés.
Prevailing Language:
In the event of any discrepancy between the English original version of this report and the Spanish language translation, the English version prevails.

División de Gestión de Riesgos, Seguridad y Cumplimiento del Servicio de Información y Tecnología (ITS, por sus siglas en inglés)
CIUDAD DE DALLAS

City of Dallas

Revisión del documento

Artículo	Descripción del cambio	Versión	Fecha	Estado del documento
1	Esquema del documento inicial	0.01	9/13/2021	PROYECTO
2	Proyecto de documento con un esquema actualizado	0.02	9/23/2021	PROYECTO
3	Proyecto de documento revisado con recomendaciones	0.03	9/29/2021	PROYECTO
4	Informe inicial	1.00	9/30/2021	Final

Informe de análisis de pérdidas de datos, agradecimientos:

El Director Financiero de la Ciudad de Dallas y el Director del Departamento de Servicios de Información y Tecnología (ITS, por sus siglas en inglés) reconocen y agradecen a la División de Gestión de Riesgos, Seguridad y Cumplimiento de ITS y a los elementos de otras divisiones de ITS por sus esfuerzos en la captación, el análisis y la elaboración de informes sobre la información y los acontecimientos relacionados con los eventos de pérdida de datos de la Ciudad de Dallas de marzo de 2021. Sin su ayuda, experiencia y antecedentes en asuntos de seguridad informática y cibernética, la Alcaldía no tendría la oportunidad de comprender en detalle las causas y los efectos relacionados con este evento.

Información general de la fuente, agradecimientos:

La Ciudad de Dallas reconoce y agradece las numerosas fuentes de información que han contribuido a la elaboración de este documento. Algunas fuentes de información se han obtenido a través de los servicios de investigación de Gartner y Forrester. La Alcaldía reconoce y agradece a estas organizaciones la orientación y asistencia que sus servicios individuales contratados proporcionan a la Ciudad. Algunas fuentes de información también se obtuvieron de elementos del Gobierno de los Estados Unidos, como el Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés), el Departamento de Seguridad Nacional y el Departamento de Justicia, entre otros. La Alcaldía reconoce y agradece a estas organizaciones la orientación y asistencia que sus servicios y marcos normativos han proporcionado a la Ciudad.

Dado que este documento no es un trabajo académico, no se utilizan citas detalladas. En general, este documento citará las fuentes de información utilizadas en la elaboración de este informe utilizando un artificio de corchetes. El artificio utilizado son los corchetes con la indicación de la fuente dentro de los corchetes. La siguiente es una ilustración de una cita utilizada en este documento: [Fuente], y [Fuente1, Fuente2].

Resumen ejecutivo

El objetivo de este documento es identificar los factores directos, contribuyentes y sistémicos relacionados con los eventos de pérdida de datos de marzo de 2021 ocurridos en la Ciudad de Dallas. El informe también esboza una serie de recomendaciones que mejorarán la gestión de los datos electrónicos por parte de la ciudad para reducir la probabilidad de que se produzcan estos sucesos en el futuro.

El primer evento, ocurrido a finales de marzo de 2021, incluía 22 Terabytes (TB) de datos, de los cuales 14,49 TB se recuperaron gracias a la ayuda de Microsoft. Los 7,51 TB posteriores se eliminaron y se consideran irrecuperables. Estos datos consisten en imágenes archivadas, videos, audios, notas de casos y otros elementos recogidos por el Departamento de Policía de Dallas. Los datos desaparecidos, a menudo denominados disco "K", resultaron la pérdida de 4,1 millones de archivos.

El segundo incidente se descubrió como resultado de que ITS realizara una auditoría exhaustiva de los 26 servidores de archivos. ITS, en colaboración con el proveedor de copias de seguridad (Commvault), ha completado una auditoría técnica de esos archivos perdidos, que ha dado como resultado una pérdida adicional de 13,167 TB. Esta pérdida adicional estaba asociada a los servidores Fusion.

Ubicación	Volumen de la Pérdida	Número de archivos
K Drive	7.51 TB	4,.1 millones de archivos
Servidor Fusion	13.167 TB	4.6 millones de archivos
Servidor CAPERS	N/A	No hay pérdida de datos
Secretario de la Ciudad	N/A	No hay pérdida de datos

Posteriormente, ITS ha aportado herramientas forenses de recuperación de datos, experiencia y personal de apoyo para escanear y recuperar datos de toda la infraestructura tecnológica de la Ciudad

de Dallas para recuperar potencialmente los datos borrados, posiblemente almacenados en fuentes alternativas. La oficina del Fiscal del Distrito y el DPD están proporcionando continuamente a ITS una lista de casos prioritarios en los que buscar para los esfuerzos de recuperación. ITS está utilizando estas herramientas y procesos forenses especializados para recuperar datos de fuentes alternativas como ordenadores portátiles, cámaras y otros dispositivos.

Además, se ha creado un entorno de recuperación en el que se pueden restaurar copias forenses de los sistemas afectados con copias de seguridad que se utilizarán en nuestros esfuerzos de búsqueda. ITS está buscando los datos perdidos en todo el entorno local y en la nube de la Alcaldía, incluyendo Microsoft Office 365, correo electrónico, SharePoint y OneDrive. Comprendemos la magnitud y la gravedad de la situación y seguiremos trabajando con diligencia con el DPD para recuperar tantos datos como sea posible. Hasta la fecha, el equipo de recuperación ha recuperado 140,353 archivos potenciales que fueron eliminados.

Tipo de datos	Saldo inicial basado en el análisis	Procesado hasta la fecha	Porcentaje de finalización
Número de casos estimados	17,494	142	8.1%
Casos prioritarios del fiscal	1,000	142	14.2%
Posibles archivos de datos	17,291,140	140,353	8.12%
Tamaño del almacén	8,3 TB		

Los factores claves que conducen a la pérdida de datos son:

- Controles de gestión inadecuados para las actividades de gestión de datos
- Insuficientes sistemas de control de gestión y supervisión del personal dentro de la división de Servicios de Infraestructura de ITS
- Insuficiente revisión y cumplimiento de los detalles de las solicitudes de gestión de cambios de la empresa relacionadas con los entornos de producción de la Alcaldía.

De este análisis se desprenden varios puntos clave:

- Algunos datos se pierden y no son recuperables (es decir, los datos se pierden permanentemente).
- Otros datos se introdujeron previamente en los sistemas que apoyan los procesos de la Alcaldía (por ejemplo, la persecución de los delitos no municipales por parte de la Ciudad) y siguen estando disponibles para la Alcaldía y sus socios comerciales (por ejemplo, el Fiscal del Condado de Dallas).

Correcciones que hay que abordar:

- La división de Servicios de Infraestructura de ITS continúa realizando cambios sin la debida autorización o aprobación, causando inestabilidad en el entorno de producción de la Alcaldía.
- La división de Servicios de Infraestructura de ITS debe implementar y operar apropiadamente sistemas de control de gestión adecuados, incluyendo sistemas de gestión de activos e inventarios.
- ITS debe implementar y operar adecuadamente los procesos de gestión de servicios de TI para eliminar la dependencia del correo electrónico y las comunicaciones de voz para procesar las solicitudes.
- Las divisiones de ITS deben implementar y gestionar adecuadamente los catálogos de Servicios Técnicos y Empresariales que identifican y definen los servicios y actividades que ITS ofrece a los departamentos y oficinas de la Alcaldía.
- ITS debe mejorar sus directivas ambientales, de gestión y operativas, así como las expectativas documentadas para generar una prestación de servicios de calidad por encima de los plazos actuales.
- ITS debe implementar y operar sistemas adecuados de control de la gobernanza y la gestión de datos para mejorar el uso, la gestión y la protección de los datos de la Alcaldía.

Gobernanza y gestión de datos: El Departamento de Servicios de Información y Tecnología (ITS) y su predecesor, el Departamento de Comunicaciones y Servicios de Información (CIS), han aplicado procesos y procedimientos inadecuados de gobernanza y gestión de datos. El marco de gobernanza y gestión de datos seleccionado por ITS es utilizado eficazmente por muchas organizaciones. Sin embargo, la anterior dirección ejecutiva de ITS no quiso o no pudo identificar y aplicar adecuadamente los procesos y procedimientos de este marco para la gestión de datos. La dirección ejecutiva de ITS ha

hecho hincapié en la necesidad de implantar y aplicar fielmente los procesos y procedimientos de gobernanza y gestión de datos para mitigar el riesgo de futuras pérdidas de datos.

Este informe se basa en la información generalmente disponible relativa a los marcos y normas de una variedad de organizaciones que incluyen agencias del gobierno federal, casas de investigación comercial y organizaciones de normas profesionales. Los organismos federales incluyen, entre otros, el Instituto Nacional de Normas y Tecnología (NIST), el Departamento de Seguridad Nacional (DHS) y el Departamento de Justicia (DOJ). Las casas de investigación comercial incluyen Gartner, Inc. y Forrester, Inc. Las organizaciones profesionales de normalización incluyen, entre otras, a Axelos, Inc., proveedora de la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) y de la versión 3 de ITIL adoptada por la ciudad (ITILv3), y a Data Management (DAMA) International, proveedora del Data Management Body of Knowledge (DMBOK).

Este informe se elaboró utilizando la información que pusieron a disposición de los autores la dirección de ITS, los altos directivos de ITS, el personal de ITS, el personal del Departamento de Policía de Dallas, el personal de la Oficina del Secretario de la Ciudad, el proveedor de software de respaldo y los profesionales expertos externos traídos a la Ciudad para ayudar en el evento de pérdida de datos. Las condiciones identificadas, las causas, el criterio, los efectos y las recomendaciones para cada factor reportado podrían cambiar si se proporciona, descubre o divulga información adicional.

City of Dallas

Índice de contenidos

City of Dallas

Sección I- Evento de pérdida de datos

Esta sección proporciona información general relativa a los eventos de pérdida de datos de marzo de 2021 en la Ciudad de Dallas.

1 Introducción

A finales de marzo de 2021, la Ciudad de Dallas sufrió una gran pérdida de datos de archivo almacenados en un servicio contratado en la nube. La pérdida de datos de archivo se produjo al migrar los datos del servicio proporcionado en la nube a un sistema de soporte de archivo de datos in situ que se mantiene para conservar los datos a largo plazo. La pérdida de datos afectó a varios sistemas operativos de la Ciudad, principalmente al Departamento de Policía de Dallas (DPD). En la actualidad, la Ciudad ha identificado una pérdida estimada de 7,51 TB de datos comprimidos, con un aproximado de 4,1 millones de archivos, y un segundo incidente identificado de 13,41 TB y 4,6 millones de archivos adicionales de pérdida de datos. El resultado es una pérdida total de 8,262 millones de archivos perdidos en el evento.

1.1 Estado de los datos de archivo

Los datos de archivo son información histórica que se mantiene con fines de gestión de registros a largo plazo. Los datos de copia de seguridad, en cambio, son una copia de los datos operativos actuales o recientes creada para facilitar la restauración de los datos de un sistema a un estado actual o reciente. Los datos operativos son los que se mantienen dentro de un sistema para permitir su funcionamiento diario y la presentación de la información.

Los datos de archivo asociados al evento de pérdida de datos de 2021 han sido eliminados permanentemente del sistema de archivo in situ de la Ciudad y no están disponibles para su recuperación dentro de ese sistema. Los datos de este incidente se presumen borrados e irrecuperables. Sin embargo, se están realizando esfuerzos para recuperar copias o duplicados de los datos de otros sistemas donde estén disponibles. Durante el curso de la revisión y el procesamiento, los datos suelen duplicarse, trasladarse y transferirse varias veces antes de quedar archivados.

1.2 Eventos de pérdida de datos

La pérdida de datos descrita en este informe se compone de dos incidentes identificados por separado. El primero de estos incidentes se descubrió a principios de abril de 2021 y fue el resultado de errores cometidos en la migración de datos desde un servicio proporcionado en la nube a un archivo de datos in situ.

Posteriormente, mientras ITS realizaba su auditoría de pérdida de datos, siguiendo el Plan de Respuesta a Incidentes, se identificó un incidente de pérdida de datos adicional. Algunas de las pérdidas de datos adicionales están relacionadas con el incidente original, otras son nuevas. Esta sesión informativa es para revisar las áreas adicionales de preocupación. Commvault e ITS siguen analizando el entorno de la Ciudad de Dallas para determinar dónde puede producirse cualquier impacto.

- El jueves 26 de agosto de 2021 se abrió un ticket de incidencia del proveedor (Commvault) (210815-92).
- El billete era una alerta, para la Ciudad, por una posible irregularidad en el almacenamiento de los archivos de datos.
- ITS se comprometió con una respuesta para triar inmediatamente la alerta, con el Director de Seguridad de la Información (CISO), el Subdirector de Servicios de Infraestructura (AD) de ITS, el Gerente de Soporte de Servidores y el Gerente de Relaciones Comerciales (BRM) de DPD, para determinar la gravedad del nuevo incidente. La evaluación, a partir del triaje, requirió la participación de los ingenieros de soporte de Commvault.
- ITS proporcionó a los ingenieros de soporte de Commvault los registros y las políticas de archivo para que los analizaran, revisaran y evaluaran.
- Los resultados de la evaluación inicial se discutieron (CISO, AD de Servicios de Infraestructura de ITS, Gerente de Soporte de Servidores, y el BRM de DPD, y Commvault) el viernes 27 de agosto de 2021, y luego se comunicaron a los Ejecutivos de ITS.

1.3 Esfuerzos de control de costos

Al revisar los acontecimientos que condujeron a la pérdida de datos, la información disponible indica que la migración de datos planificada a finales de marzo de 2021 desde el servicio proporcionado por la nube al archivo de datos in situ formaba parte de un esfuerzo por reducir los costos de datos asociados de la Ciudad.

En 2015, la Ciudad de Dallas contrató a Microsoft para los servicios en la nube de Azure en virtud de la Resolución del Concejo 15-1049. El departamento de Servicios de Comunicación e Información (CIS) presentó la iniciativa de iniciar el proceso de migración a la nube para trasladar las cargas operativas digitales de los centros de datos locales de la Ciudad a una "presencia en la nube". "La estimación del costo de los gastos en la nube se había reconocido en 60,000 dólares al año para aprovechar el

almacenamiento híbrido de Azure (Storsimple). Además, en 2018 el Ayuntamiento previó un gasto adicional por una conexión de "ruta exprés" para reducir la latencia de la red y los servicios de datos rápidos a Azure. Posteriormente, estos costos no habían sido renegociados ni presentados a concurso para evaluar y optimizar las estimaciones de control de costos de los servicios en la nube.

En 2019, con los cambios en la gestión de ITS, los Servicios de Información y Tecnología de la Ciudad de Dallas (ITS) tuvieron un gasto de 908.000 dólares asociado a los servicios en la nube de Azure. En ese momento, se estimaba que un 5% de la carga de trabajo de la Ciudad se había migrado a la nube. En 2020, la carga de trabajo se había incrementado hasta un 10% aproximadamente, con un aumento del gasto de 1,8 millones de dólares. Posteriormente, en 2021 la Ciudad tenía un gasto mensual aproximado de 122.000 dólares, que superaba el gasto en la nube más allá de los 100.000 dólares mensuales previstos. Mientras que en 2021, esa carga de trabajo se había reducido al 7% de los servicios de TI.

Las estrategias de migración a la nube deben ser un proceso bien definido y adecuadamente evaluado antes de su implementación. Los esfuerzos de migración inteligente a la nube evalúan las opciones disponibles en función de las necesidades del servicio y la misión, los requisitos técnicos y la política. Las decisiones de procesamiento y tecnología deben considerar el impacto en el cliente frente a los criterios de gestión de costos y riesgos de ciberseguridad. Deben tenerse en cuenta cálculos como los requisitos del servidor, el ancho de banda de la red y los recursos de la aplicación. [Gartner]

Antes de llevar a cabo una migración a la nube es necesario realizar un análisis y un diseño arquitectónico completos. Además, los costos asociados a las soluciones basadas en la nube incluyen la computación, el almacenamiento y la transferencia de datos. En consecuencia, esas estimaciones deben traducirse en una expectativa de Costo negociada con el proveedor. Estos requisitos básicos y la aplicación de los principios de la nube no se llevaron a cabo adecuadamente, salvo en lo que respecta a los supuestos beneficios de la nube. [Gartner, ITILv3]

Las responsabilidades fiscales y las acciones de asignación de ingresos fiscales imponen una gran carga de responsabilidad a la Alcaldía para garantizar que se desarrollen estimaciones de costos adecuadas utilizando un modelo de gasto realista y preciso [Libro Verde de la GAO]. Se comunicó que antes del intento de migración de datos y de la posterior pérdida de datos, ITS realizó una revisión de sus patrones de gasto con respecto al presupuesto asignado actual, mostrando una métrica de gasto insostenible. También se comunicó que, como resultado del análisis de los gastos, la dirección de ITS

decidió devolver ciertas cargas de trabajo a un modelo de almacenamiento local más controlado en cuanto a costos, a pesar de que no se habían realizado evaluaciones de riesgo adecuadas.

Al considerar la necesidad de una implementación más controlada de los Costos, la dirección de ITS debería haber identificado todos los riesgos potenciales. [NIST] En ningún momento los recursos técnicos y de gestión evaluaron los riesgos técnicos y de Costos en relación con las mejores prácticas.

Según el Instituto Nacional de Estándares y Tecnología (NIST), varios riesgos elevados incluyen la pérdida de datos en grandes volúmenes durante los traslados entre entornos y las considerables interrupciones de los procesos en toda una organización. Para evitar impactos perjudiciales para la organización, los departamentos de TI deben considerar un plan de recuperación de desastres exhaustivo en caso de que los datos desaparezcan. [NIST]

De acuerdo con las mejores prácticas del NIST y las directrices de Microsoft Azure, no se definieron ni se aplicaron procedimientos adecuados de copia de seguridad o de recuperación de desastres para una migración de gran volumen a fin de evitar esta pérdida de datos. [Según las mejores prácticas de uso de la nube de Microsoft, ITS debe mantener múltiples métodos para la prevención de la pérdida de datos. Las migraciones de grandes volúmenes de datos deben estar bien planificadas y resumidas. [NIST, Azure] La supervisión técnica y de gestión clave con redundancia de pruebas y validación para cualquier migración es vital para cualquier transferencia de datos exitosa. [NIST, Azure, Gartner] Ninguna de estas medidas o validaciones se había completado o puesto en marcha en el momento de los sucesos de pérdida de datos de marzo de 2021.

Dado que las mejores prácticas de copia de seguridad y almacenamiento en la nube son fundamentales para un esfuerzo de recuperación bien equilibrado, no debe considerarse el abandono del esfuerzo en la nube. Sin embargo, la dirección de ITS debe proporcionar un análisis de Costos adecuado y un modelo de gasto presupuestario controlado. ITS debe adherirse a un modelo de mejores prácticas completando y revisando el análisis estratégico de Costos y riesgos de ese uso. Estas medidas habrían reducido en gran medida el riesgo de pérdida de datos de la migración de la disco "K". [Gartner, Azure]

1.4 Procedimiento de Incumplimiento

El proceso de copia de seguridad de la Ciudad de Dallas no cuenta con procedimientos explícitos de gestión de datos para su archivo. Por ejemplo, los procedimientos de gestión de datos deberían incluir

procedimientos para la migración de datos de archivo desde soluciones basadas en la nube a soluciones de almacenamiento de datos de archivo de la Ciudad in situ. [Los procedimientos proporcionados por el proveedor, si se siguen con exactitud, proporcionan instrucciones para migrar adecuadamente los datos de archivo de las soluciones de almacenamiento basadas en la nube de la Ciudad a soluciones de almacenamiento de archivo in situ menos costosas. Sin embargo, estos procedimientos de solución desarrollados por el proveedor no abordan las metas, los objetivos o los requisitos de la gestión de datos de la Ciudad.

La Ciudad de Dallas ha determinado que el personal de la Alcaldía no siguió fielmente los procedimientos de migración de datos de archivo proporcionados por el proveedor de software. [Además, no se ha determinado que el personal de la Ciudad en cuestión notificara a la dirección de la Alcaldía que los procedimientos eran inexactos, incompletos o incorrectos para permitir la revisión y actualización de los procedimientos de migración de datos de archivo.

Cualquier software suele tener una metodología definida (es decir, procedimientos) para utilizarlo. Estos procedimientos, especialmente cuando la eliminación de datos puede ser perjudicial para el uso y el acceso de los datos por parte de la Alcaldía o del departamento de negocios, deben ser bien comprendidos antes de tomar medidas contra un entorno de producción. En la revisión de ITS, se determinó que había un malentendido evidente o un desconocimiento de los procedimientos definidos por parte del empleado. Además, al revisar los procedimientos, ITS descubrió que el software del proveedor permite múltiples opciones para evitar la pérdida de datos durante una migración o traslado. El técnico tiene múltiples advertencias y múltiples oportunidades de cancelar y revisar el riesgo asociado a una acción antes de completar el cambio de configuración. Al revisar las acciones del técnico, parece que no hizo caso de estas advertencias.

1.5 Sistemas afectados

La Auditoría de Pérdida de Datos de ITS, siguiendo las acciones requeridas por el Plan de Respuesta a Incidentes de Recuperación de Desastres de ITS, ha identificado los sistemas de la Ciudad que sufren el impacto de estos eventos de pérdida de datos. Algunos sistemas identificados se conocieron inmediatamente después de la pérdida de datos inicial. Otros sistemas que han sufrido pérdidas de datos se identificaron tras una revisión e investigación más exhaustiva.

Los datos de archivo y copia de seguridad se han eliminado permanentemente de las soluciones de almacenamiento en la nube de la Alcaldía y de las soluciones de almacenamiento de datos de archivo in situ de la Alcaldía para los siguientes sistemas:

Oficina del Secretario de la Ciudad:

La auditoría preliminar identificó una pérdida de datos de 2.133 TB debido al borrado de los datos de las copias de seguridad en el servidor del secretario municipal. Sin embargo, tras un examen más detallado, el descubrimiento de una política secundaria proporcionó pruebas de que el técnico había duplicado la política de archivo. Posteriormente, como resultado de una investigación más profunda a través de la auditoría con el proveedor, se demostró que los datos estaban intactos.

- Todos los datos auditados como presentes.

Departamento de Policía de Dallas:

CAPERS - La auditoría preliminar identificó una pérdida de datos de 244.02 GB debido a la eliminación de datos de copia de seguridad en el servidor CAPERS. Sin embargo, tras un examen más detallado, el descubrimiento de una política secundaria proporcionó pruebas de que el técnico había duplicado la política de archivo. Posteriormente, como resultado de una investigación más profunda a través de la auditoría con el proveedor, se demostró que los datos estaban intactos.

- Todos los datos auditados como presentes.

FUSION - Entre el 20 de noviembre de 2019 y el 22 de agosto de 2020, 434 trabajos de archivo provocaron el borrado de datos del servidor FUSION. Los trabajos de archivo estaban en la unidad "F" como parte del almacenamiento para el servidor. La edad de archivo de todos los volúmenes de la unidad "F" del servidor se estableció en 10 meses. Al producirse el borrado el 31 de marzo de 2021, se eliminó cualquier archivo que no hubiera sido modificado antes del 1 de junio de 2020.

- Unidad F – 13.167 TB

Unidad "K" archivada - La migración de datos del almacenamiento en la nube del archivo a las instalaciones a finales de marzo de 2021 por una metodología inadecuada en el proceso de migración provocó la pérdida de 7.51 TB de datos. La pérdida de datos consistió en aproximadamente 4.1 millones

de archivos de múltiples divisiones del Departamento de Policía de Dallas. Sin embargo, la mayor parte de la pérdida ha afectado aparentemente a la Unidad de Violencia Familiar. Estos datos consistían en información recopilada por los detectives del DPD para casos procesables, adjudicados y en curso; o pruebas generales recopiladas.

- Unidad K – 7.51 TB

1.6 Sistemas no afectados

Tras completar una exhaustiva auditoría de revisión técnica el 27 de agosto de 2021, de todos los datos de archivo con respecto a la tecnología de archivo y copia de seguridad, se demostró que varios sistemas no han sufrido pérdidas de volumen de datos ni se han eliminado permanentemente los datos de las soluciones de almacenamiento en la nube de la Ciudad o de las soluciones de almacenamiento de datos de archivo in situ de la Ciudad para los siguientes sistemas de interés:

Departamento de Policía de Dallas (DPD): Sistema de Gestión de Registros (RMS). El sistema RMS es un sistema primario utilizado por el DPD para las pruebas digitales que luego se cargan en el Portal de la Agencia de Aplicación de la Ley Lumen.

- Todos los datos auditados como presentes.

Departamento de Bomberos de Dallas (DFR) Los sistemas de copia de seguridad y archivo de DFR son archivos compartidos proporcionados al Departamento de Bomberos de Dallas para la conservación de archivos.

- Todos los datos auditados como presentes.

Los sistemas de copia de seguridad y archivo de la Oficina del Fiscal de la Ciudad (CAO) son archivos compartidos proporcionados a la Oficina del Fiscal de la Ciudad de Dallas para la conservación de archivos.

- Todos los datos auditados como presentes.

Los sistemas de copia de seguridad y archivo de la Oficina del Interventor de la Ciudad (CCO) son archivos compartidos proporcionados a la Oficina del Interventor para la conservación de archivos, incluido el Sistema Financiero Advantage.

- Todos los datos auditados como presentes.

Los sistemas de copia de seguridad y archivo de los Servicios de Agua de Dallas (DWU) son archivos compartidos proporcionados al Departamento de Servicios de Agua para la conservación de archivos.

- Todos los datos auditados como presentes.

Los sistemas de copia de seguridad y archivo del Departamento de Aviación (AVI) son archivos compartidos proporcionados al Departamento de Aviación para la conservación de archivos.

- Todos los datos auditados como presentes.

Los sistemas de copia de seguridad y archivo del Departamento de Obras Públicas (PBS) son archivos compartidos proporcionados al Departamento de Obras Públicas para la conservación de archivos.

- Todos los datos auditados como presentes.

Los sistemas de copia de seguridad y archivo de ITS son archivos compartidos proporcionados a ITS eDiscovery para la retención de archivos.

- Todos los datos auditados como presentes.

Los sistemas de copia de seguridad y archivo de los Sistemas de Información Geográfica (SIG) son archivos compartidos que se proporcionan a los Sistemas de Información Geográfica de la DBI para la conservación de los archivos.

- Todos los datos auditados como presentes.

Los sistemas de copia de seguridad y archivo de la Iniciativa Big Data de ITS son archivos compartidos proporcionados a los sistemas de información Big Data para la conservación de archivos.

-Todos los datos auditados como presentes.

1.7 Normas y Prácticas de Tratamiento de Datos

La Ciudad de Dallas cuenta con políticas, normas y procedimientos de gobernanza y gestión de datos no desarrollados. En el sitio web externo de la Ciudad se ha publicado un documento básico de estrategia de gestión de datos. Sin embargo, el documento de estrategia de gestión de datos está desfasado y no se ha implantado como actividad y proceso formal dentro del entorno de datos de la Ciudad.

La gestión de datos existe en cierto grado en cada departamento, en función de las necesidades de cada uno de ellos. Normalmente, la gestión que existe se debe a los requisitos reglamentarios municipales, del condado, del estado o federales. Existen algunos esfuerzos para la calidad de los datos en el uso de las direcciones en todos los departamentos, pero incluso aquí hay múltiples metodologías y requisitos de direcciones.

El Ayuntamiento también carece de sistemas de control de gestión adecuados para los datos no estructurados. Hay pocos controles sobre los datos que pueden almacenarse, a menos que existan requisitos normativos específicos. Se realizan copias de seguridad de los datos no estructurados, pero rara vez se realizan pruebas de recuperación de los datos no estructurados, a menos que exista un requisito de auditoría específico para hacerlo. Rara vez, o nunca, se realiza una auditoría para garantizar que todos los datos no estructurados requeridos se respaldan mediante metodologías aprobadas. La gestión de los datos no estructurados en un entorno de nube añade dificultades que requieren conjuntos de habilidades adicionales y una supervisión que normalmente no está disponible o implementada.

El hecho de no contar con una capacidad de gestión de datos completa, centralizada y aplicada por un comité de gobernanza de datos es un factor de las condiciones que condujeron a un entorno en el que es posible la pérdida de datos. Este fallo, sobre todo en lo que respecta a los datos no estructurados, fue un factor importante, entre muchos otros, que culminó en la pérdida y la consiguiente incapacidad para recuperar los datos del Departamento de Policía de Dallas.

2 Cronología de la Pérdida de Datos

La siguiente línea de tiempo está relacionada con las eliminaciones del archivo de datos del DPD.

El técnico de copias de seguridad inició el proceso no autorizado de "Hard Delete Client", a través de Commvault, a partir del 30 de marzo y hasta el 31 de marzo de 2021.

Lunes 5 de abril de 2021 (aproximadamente a las 9:00 horas) - El técnico de copias de seguridad recibió el primero de los muchos tickets de servicio de los clientes del personal de DPD indicando archivos perdidos o inaccesibles.

Lunes 5 de abril de 2021 (aproximadamente a las 11:00 horas) - El técnico de la copia de seguridad ha cerrado todos los borrados de la biblioteca, deteniendo así el proceso de limpieza del cliente.

Lunes 5 de abril de 2021 (12:08 pm) - El técnico de copias de seguridad se puso en contacto con el soporte de Commvault para iniciar el proceso de recuperación y determinar el alcance del incidente.

Lunes 5 de abril de 2021 (aprox. 12:30 pm) - El técnico de respaldo se puso en contacto con su gerente para notificar el incidente. Se le dijo al técnico de respaldo que continuara con el esfuerzo de recuperación y que informara al gerente del alcance total.

Martes 6 de abril de 2021 (7:00 horas) - El responsable del técnico de refuerzo se puso en contacto con el Subdirector de Infraestructuras para informarle de la incidencia y del alcance del impacto conocido.

Miércoles 7 de abril de 2021 (15:30 horas) - El informe inicial indicaba que se había archivado un total de 22 TB de almacenamiento y que el técnico de copias de seguridad y el proveedor habían restaurado 11 TB de archivos en ese momento. La investigación posterior mediante el análisis de los registros ha determinado que las cantidades reales son las siguientes:

- Se archivaron 14 TB de datos desduplicados en el almacenamiento de Azure (35 TB de datos de archivos "en bruto" que no están desduplicados)
- 10,77 TB de datos fueron eliminados por los eventos del 30/3 al 31/3
- 3,26 TB de (datos recuperados)
- 7,51 TB de datos afectados (datos eliminados)

Jueves 8 de abril de 2021 (2:00 am) - Informe final del técnico de copias de seguridad mostrando el total de archivos perdidos (aproximadamente 11 TB inicialmente).

NOTA: Esta línea de tiempo representa las acciones e investigaciones para los archivos de datos perdidos del disco "K" del DPD, solamente. No incluye los servidores "CAPERS" o "FUSION".

Periodo 3/26-8/25/2021	Eventos
Martes 28/03/2021	**CA CHG Ticket 117304 - Implementar una nueva biblioteca de almacenamiento de Azure**
Miércoles 31/03/2021 17:04 PM	El 31 de marzo de 2021 a las 17:04, el técnico eliminó la política de almacenamiento de Commvault Archive. El efecto de esta eliminación fue la eliminación de todos los trabajos asociados a esa política de almacenamiento. La eliminación afectó a cinco servidores: servidor. Además, se eliminó el índice de almacenamiento. La investigación inicial se ha centrado en los servidores.
Martes 04/06/2021 9:27 AM	El BRM de ITS del DPD y el Subdirector de Infraestructura de ITS notificaron al CIO.
Vie. 04/09/2021	El CIO y el CFO discutieron el tema de la pérdida de datos
Martes 13/04/2021 14:53	El CIO notificó a la dirección de la Ciudad: "El propósito de este correo electrónico es informarle de una pérdida masiva de datos que se ha producido debido a un error durante la realización de las transferencias rutinarias de archivos desde el almacenamiento de Azure al almacenamiento del Ayuntamiento de los archivos del DPD", "Estamos preparando una reunión con el Jefe Martínez y el Jefe Schultz esta tarde".
Miércoles 14/04/2021	Reunión con la dirección del DPD y el BRM del DPD de ITS
Período 26/08/2021	**Eventos**
Jue. 26/08/2021 18:25 PM	El CISO activó el PIR para el análisis de la pérdida de datos
Jue. 26/08/2021 18:28 PM	El gestor de incidentes se puso en contacto con el subdirector
Jue. 26/08/2021 18:30 PM	El gestor de incidencias organiza una reunión de equipos
Jue. 26/08/2021 18:35 PM	P1 Ticket abierto - Posible política de almacenamiento eliminada de todos los departamentos - 31 de marzo de 2021 - Commvault notificó al CdD el 26/8/21
Jue. 26/08/2021 18:45 PM	Triaje: Liderazgo de ITS
Jue. 26/08/2021 18:57 PM	Gerente para llegar a Commvault - verificando que los datos del arco
Jue. 26/08/2021 19:05 PM	Ticket de Commvault 210815-92
Jue. 26/08/2021 19:25 PM	Triaje con Commvault Supt - Seguimiento de ETA 23:30 pm Commvault seguir
Jue. 26/08/2021 23:30 PM	Llamada de estado de Commvault
Vie. 27/08/2021 07:30 AM	Actualización del análisis de pérdida de datos
Vie. 27/08/2021 07:35 AM	Comunicación de la situación al CISO/CIO
Vie. 27/08/2021 08:05 AM	Revisar la matriz de evaluación con el AD

Vie. 27/08/2021 08:35 AM	Revisar la matriz de evaluación con el CISO
Vie. 27/08/2021 09:00 AM	Revisar la matriz de evaluación con el CIO
Vie. 27/08/2021 13:30 PM	Revisar la matriz de evaluación con la dirección de la Ciudad
Vie. 27/08/2021 14:15 PM	Se ha contactado con la Dirección de Infraestructuras en relación con los artefactos para la Secretaría de la Ciudad y el RMS
Vie. 27/08/2021 15:30 PM	Reunión con la Secretaría de la Ciudad
Vie. 27/08/2021 16:05 PM	La notificación formal de la posible pérdida de datos se envió a la OCM, a la Alcaldía, al Concejo y a la Fiscalía.
Vie. 27/08/2021 16:25 PM	La Secretaría de la Ciudad se dio cuenta de que pueden tener una copia separada de su Archivo 2019
Vie. 27/08/2021 16:30 PM	Reunión con Commvault para conocer la situación de la Secretaría Municipal y el RMS
Vie. 27/08/2021 17:57 PM	Actualizaciones de Commvault proporcionadas al CIO
Vie. 27/08/2021 21:00 PM	Reunión con la dirección de ITS
Lun. 30/08/2021 09:50	Gestión de la infraestructura - Trabajo con Commvault para crear una herramienta de identificación, para identificar los talones. ETA COB 9/1
Lun. 30/08/2021 17:30 PM	Revisar las actividades diarias
Mie. 09/01/2021 17:30 PM	Progreso de la herramienta de identificación - En progreso, BRM proporcionará el cumplimiento de los próximos casos de DA - Completado; Reunión de inicio del miércoles con Birch Cline Consulting https://www.birchcline.com especialista en datos recuperación de datos como la rehidratación
Jue. 09/02/2021 17:30 PM	El director del servidor confirmará la pérdida de datos real de City Security - posibilidad de archivo adicional - el CIO querría para el COB; la lista está en proceso para el servidor. A la espera de la comunicación de la SEC; reunión de actualización de Commvault para las 8 de la mañana del 3 de septiembre
Jue. 09/02/2021 21:45 PM	(CO) órdenes de cambio enviadas al Gerente Principal de Cumplimiento
Mar. 09/07/2021 08:30 AM	Scripts de Commvault: No hay novedades. El tiempo estimado de llegada es el 9/7, a la espera de la respuesta de Commvault; el tiempo estimado de recogida de pruebas es el viernes 9/10; dos recursos GTS han comenzado hoy, 9/7 - 22k de correo electrónico; el almacenamiento est. ETA prevista <5-10d>
Jue. 09/09/2021 08:30 AM	Revisar las actividades diarias
Sáb. 09/11/2021 11:00 AM	Los técnicos están en camino de reunirse con Hitachi en el Ayuntamiento a las 11 de la mañana; un técnico está a la espera de hacer la copia en bits al Hitachi una vez que se haya puesto en marcha a última hora de la tarde/principios de la noche; informaré a BRM para que esté preparada para informar a DPD de nuestro calendario actual; los técnicos están a la espera de hacer la copia en bits alternativa con las unidades USB que se adquirirán/entregarán hoy; en cualquier caso, deberíamos estar preparados para empezar la copia en bits a primera hora de la tarde como muy tarde.

Sáb. 09/11/2021 18:11 PM	Vamos a repartir la imagen Fusion entre dos unidades; el técnico debería empezar en breve, si no lo ha hecho ya; la instalación de Hitachi está en curso. Tenemos un pequeño problema con los conmutadores Brocade. Ahora estoy trabajando en ello, pero el sistema que he instalado se ha puesto en marcha y la configuración está en marcha.
Sáb. 09/11/2021 18:27 PM	El controlador de almacenamiento está configurado de la mejor manera posible por Hitachi; Hitachi creó 4 Luns de 10 TB cada uno (40 TB en total) y los asignó a los puertos como Lun # 10 - 13; Conectó los cables a los conmutadores Brocade existentes; Podemos "ver" los wwns de otros servidores desde el lado del almacenamiento, por lo que la conexión al Brocade es buena para las 4 rutas; Sin embargo, no pudimos iniciar sesión en los Brocades para hacer la zonificación, así que ahí es donde se encuentra. El lado del almacenamiento es bueno ahora; Para las unidades USB - el técnico declaró que el proceso de copia de datos al formato de imagen *.E01 se ha iniciado y está en marcha. El tiempo estimado de finalización aún no ha sido devuelto por la herramienta, enviará una actualización con esa información tan pronto como esté disponible.
Dom. 09/12/2021 12:12 PM	De parte del técnico: Parece que aún nos quedan aproximadamente 52 horas, el ritmo de copias es más lento de lo previsto; estamos en torno al 25% esta mañana, al ritmo actual nos encontramos en algún momento del martes por la mañana; seguiré vigilando y les informaré si algo cambia.
Lun. 13/09/2021 17:30	Reunión de Microsoft el 10 de septiembre - Proceso de escaneo, almacenamiento, rehidratación - depende de la finalización de la clonación; guión de Commvault el 10 de septiembre - DPD y Oficina del Secretario de la Ciudad - Actualización una vez que se haya completado la clonación - martes por la tarde el 14 de septiembre; Commvault legal el 10 de septiembre - Declaración - completada; Retirada de los Servidores Fusion - En progreso - ETA el martes por la tarde el 14 de septiembre; Hitachi walk-thru - 90% completado el 11 de septiembre; CISO - Ha contratado a un proveedor para tamizar los datos más rápidamente; CISO - Marco del informe iniciado para la complejación del 30 de septiembre.
Mié. 15/09/2021 17:30 PM	Recorrido de Hitachi - Completado el 11 de septiembre; Guión de Commvault el 10 de septiembre - Departamento de Policía y Oficina del Secretario de la Ciudad - Actualización una vez que se haya completado el clon - Hora de clonación el martes por la tarde el 14 de septiembre; El técnico recogerá el USB el jueves 16 de septiembre; Reunión de Microsoft - Proceso de escaneo, almacenamiento, rehidratación - depende de que se complete el clon; Commvault legal - Declaración - completada el 13 de septiembre; Retirada de los servidores Fusion - Completada el 14 de septiembre; CISO - Ha contratado a un proveedor para revisar los datos más rápidamente - Reunión de seguimiento para el 16 de septiembre; Actualización de Commvault CRB el 16 de septiembre - La fecha prevista para la actualización es el 19 de septiembre; CISO - Marco de informes iniciado para la complejación de los informes el 30 de septiembre - Borrador de ETA para el 16 de septiembre;
Modo de recuperación	

City of Dallas

Sección II- Factores que Influyen Directamente en la Pérdida de Datos

Los eventos de pérdida de datos de marzo de 2021 de la Ciudad de Dallas se ven directamente afectados por los siguientes factores presentes en el Departamento de Servicios de Información y Tecnología (ITS) de la Ciudad de Dallas:

3 Documentación de requisitos y procesos de evaluación de riesgos

La documentación y la evaluación de riesgos son componentes críticos de las mejores prácticas para la gestión de cambios en un entorno de tecnologías de la información (TI). Permiten comprender y orientar a un técnico sobre los riesgos potenciales y posibles asociados a una solicitud de cambio, así como definir la criticidad de los datos y la actividad o el proyecto. Las direcciones administrativas y las normas de la Ciudad de Dallas se publican para proporcionar orientación y guía sobre cómo realizar un cambio. Sin embargo, la criticidad de los cambios y las evaluaciones de riesgo deben completarse y articularse con el liderazgo y el negocio para comprender plenamente los riesgos asociados con el cambio.

Al revisar la migración de datos planificada, el técnico de ITS que participó en la pérdida de datos no evaluó ni documentó suficientemente el riesgo potencial de este cambio. Esto fue un factor directo y contribuyente a la pérdida de datos. Aunque había documentación, ésta describía sobre todo los componentes de la arquitectura e información concreta sobre dónde residiría la migración de datos. Según ITILv3, un marco de mejores prácticas para la gestión de servicios de TI adoptado por el departamento de TI de la Ciudad en 2010, la documentación exhaustiva debe incluir:

- Costo-beneficio (Costo-eficacia)
- Disponibilidad de recursos
- Riesgos identificados
- Repercusión en otros servicios e impacto empresarial
- Requisitos de cumplimiento (si los hay)

Tres gerentes de los Servicios de Infraestructura de ITS revisaron la solicitud de cambio que condujo a los eventos de pérdida de datos de marzo de 2021. Para ello, los gestores de los Servicios de Infraestructura de ITS o bien no comprendieron las acciones que debían realizarse, el riesgo potencial de fracaso, o bien revisaron de forma negligente la solicitud de cambio antes de dar su autorización y aprobación para proceder a la misma.

La dirección ejecutiva y la alta gerencia de los ITS deben comprender la necesidad de documentar los procesos y de realizar una evaluación exhaustiva de los riesgos, especialmente en el caso de las actividades poco frecuentes y de alto riesgo. ITILv3 proporciona categorías y dirección para la documentación. La dirección ejecutiva y la alta gerencia de ITS deben establecer claramente el tono

ambiental apropiado a través de directivas documentadas y expectativas de desempeño para que todo el personal entienda que las acciones tienen repercusiones y que se deben tomar las actividades apropiadas de mitigación de riesgos para asegurar que se logren los resultados deseados del negocio. Por último, en lo que respecta a este tema, la dirección ejecutiva y la alta gerencia de ITS deben llevar a cabo una supervisión exhaustiva de la evaluación de riesgos para garantizar que las actividades apropiadas y adecuadas se lleven a cabo de forma que se reduzcan los riesgos.

4 Los planes de Implantación de Soluciones no se Ejecutan Fielmente

Commvault proporcionó a la Ciudad documentación detallada sobre los procesos y procedimientos necesarios para trasladar eficazmente los datos entre entornos (por ejemplo, Microsoft Azure y las soluciones de archivo de datos alojadas en la Ciudad). Microsoft Azure proporciona además un proceso de mejores prácticas y declaraciones de procedimientos para esos tipos de movimientos. La Dirección Administrativa 2-28 de la Ciudad y los procesos y procedimientos de ITILv3 relativos a la gestión de cambios también requieren planes de implementación detallados y planes de respaldo. El desarrollo o el uso de planes y procedimientos de implementación deficientes aumentan la probabilidad de que se produzcan fallos durante el despliegue.

El técnico que implementó la solución no siguió los procedimientos de migración de datos del proveedor ni las mejores prácticas identificadas para el manejo o la migración de datos. Según la documentación de procedimiento del proveedor, el técnico no cumplió con las prácticas de migración de datos detalladas por Commvault y aceptadas por la Ciudad.

La dirección de ITS no supervisó suficientemente la migración teniendo en cuenta la importancia de los datos. La supervisión inadecuada y la desviación de los procedimientos contribuyeron directamente a la pérdida de datos de la Ciudad en marzo de 2021. Una vez más, los procesos y procedimientos de ITILv3 requieren planes de respaldo debidamente detallados para garantizar la integridad y el funcionamiento de un entorno de producción. Los requisitos de procesos y procedimientos internos y externos no pueden ignorarse sin aumentar el riesgo para el entorno de producción de la Ciudad.

La dirección ejecutiva y la alta gerencia de ITS deben tomar ciertas medidas organizativas para evitar futuras pérdidas de datos de este tipo. El liderazgo debe inculcar un sentido de integridad mediante un tono organizativo adecuado. La dirección ejecutiva y la alta gerencia de ITS deben detener los despliegues en caso de fallo del guión de despliegue y comenzar la ejecución de los planes de retirada. La dirección ejecutiva de ITS y la alta dirección deben seguir fielmente los planes de retirada para garantizar la seguridad del entorno de producción de la Ciudad.

5 Controles de Gestión de Acceso

La Gestión de Identidades y Accesos (IAM) es un marco de políticas y tecnologías para garantizar que los usuarios adecuados tengan un acceso apropiado a los recursos tecnológicos. Las prácticas de IAM ayudan a una organización a identificar, autenticar y controlar el acceso de los individuos que utilizan los recursos tecnológicos. El acceso a los recursos tecnológicos por parte de los individuos y/o sistemas se controla a través de la definición y aplicación de las cuentas por las que se concede el acceso. Las Cuentas de Servicio son cuentas que son utilizadas por el software (normalmente en un servidor) para llevar a cabo tareas automatizadas como la ejecución de copias de seguridad. Las cuentas de usuario son utilizadas por el personal en su trabajo diario para acceder a un ordenador y realizar sus tareas. Las cuentas de administrador generalmente proporcionan los niveles más altos de acceso, a menudo permitiendo al usuario cambiar la configuración de seguridad, instalar y configurar el software y cambiar los permisos en otras cuentas de usuario. Las cuentas de servicio sólo deben proporcionar los permisos mínimos necesarios para los servicios necesarios del sistema para evitar posibles daños o pérdidas de datos.

El área de publicaciones especiales del NIST define los controles de gestión de acceso, los procesos de los sistemas y los procedimientos. Además, la Ciudad de Dallas tiene una definición de normas para diferentes cuentas, como las de servicio, de usuario y administrativas. La definición del área de práctica amplía y discute las prácticas de gestión y control de acceso que se describen en NIST 800-53 Controles de Seguridad y Privacidad para Sistemas de Información y Organizaciones y son las normas adoptadas por la Ciudad. Microsoft proporciona una guía para revisar y reducir el número de cuentas en grupos administrativos altamente privilegiados.

Además, todas las actividades realizadas bajo un administrador deben ser rastreadas y asignadas a la cuenta administrativa. En el caso de los sucesos de pérdida de datos de marzo de 2021, los registros del sistema están vinculados a cuentas de usuario administrativas en lugar de a una cuenta de servicio "propiedad" del servicio, lo que constituye un uso indebido de una cuenta de administrador y de los privilegios para gestionar la aplicación. En este caso, se viola el concepto de acceso de mínimo privilegio. Esta violación del uso de la cuenta pone de relieve la mala gestión de las cuentas por parte del técnico y fue un factor en el evento de pérdida de datos de marzo de 2021. Además, cuando un técnico se marcha, este mal uso de las cuentas puede causar interrupciones en los servicios de los procesos de

copia de seguridad y almacenamiento vinculados a la cuenta. Estas acciones crearon lagunas en el proceso de copia de seguridad que podrían haber causado daños adicionales en las copias de seguridad y los archivos. El personal de la Ciudad no debe utilizar las cuentas de administrador para operar los servicios como ocurrió en este caso.

6 Procesos de Contratación y Gestión de Proveedores

El proceso de gestión de proveedores garantiza que los proveedores, la tecnología y los servicios que prestan se gestionan para respaldar los objetivos de servicio de TI de la Ciudad y las expectativas empresariales. La gestión de proveedores plantea riesgos en dos ámbitos. En primer lugar, según el Departamento de Seguridad Nacional, los proveedores suponen un riesgo adicional para la Ciudad al permitir el acceso externo a los sistemas que soportan la infraestructura. Además, la Ciudad pasa a depender del proveedor para el soporte de los servicios que ITS proporciona a los departamentos de la Ciudad. El objetivo de la gestión de los proveedores es proporcionar servicios adicionales en los casos en que existan lagunas de conocimientos y un servicio de apoyo para la asistencia de los recursos. La dependencia excesiva de la gestión del servicio y del sistema por parte del proveedor se limita a las obligaciones contractuales y es difícil de adaptar a las necesidades adicionales o a los cambios en el entorno.

El objetivo del proceso de gestión de proveedores es obtener valor en relación con el Costo de los proveedores, así como garantizar el cumplimiento del contrato y los acuerdos, respetando todos los términos y condiciones.

Los principales objetivos del proceso de gestión de proveedores son:

- Garantizar que los contratos y acuerdos con los proveedores se ajusten a las necesidades de la empresa.
- Apoyar y alinearse con los objetivos acordados en los Requisitos de Nivel de Servicio y los Acuerdos de Nivel de Servicio.
- Gestionar las relaciones con los proveedores.
- Gestionar el rendimiento de los proveedores.
- Mantener una política de proveedores y un contrato de apoyo a los mismos.

El departamento de ITS depende en gran medida de los proveedores para la prestación de soluciones de servicio a los sistemas empresariales de la Ciudad. La dirección ejecutiva y superior de ITS debe haber identificado el alcance y los requisitos incluidos en las negociaciones contractuales antes de la implementación de los servicios. La gestión de los contratos debe obligar a los proveedores a cumplir con parámetros de rendimiento mensurables. Además, el personal de ITS debe tener las habilidades

suficientes para abordar los problemas de conflicto entre el proveedor y la Ciudad, con una comprensión total de los sistemas. En última instancia, ITS es responsable de los sistemas gestionados por los proveedores y debe garantizar que los procesos y procedimientos se ajusten a esa responsabilidad del proveedor.

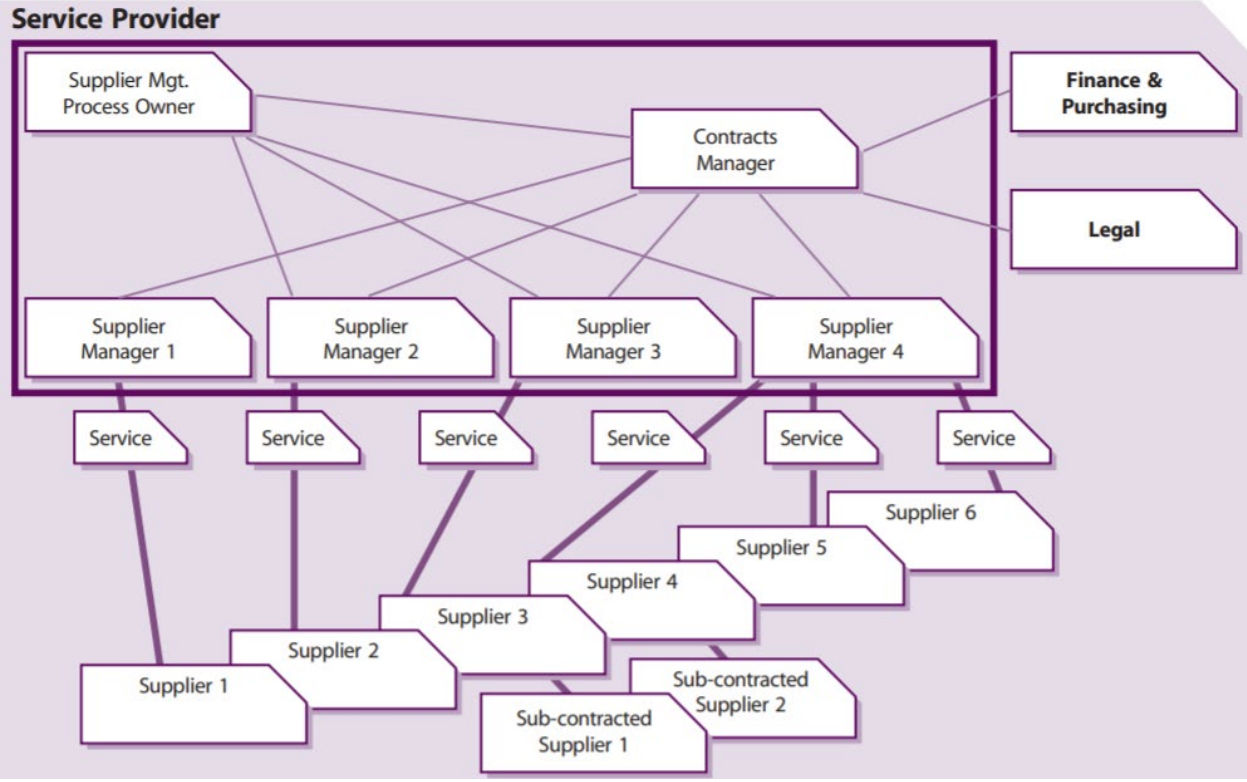


Figura 1Gestión de proveedores de ITILv3 - Roles e interfaces

City of Dallas

Sección III- Factores que Contribuyen a la Pérdida de Datos

Se han identificado los siguientes factores que han contribuido a los eventos de pérdida de datos de marzo de 2021.

7 Gobernanza y Gestión de Datos

La gobernanza y la gestión de los datos proporcionan dirección y orientación para la conservación y el tratamiento de los datos. La Ciudad de Dallas no ha hecho hincapié en la gobernanza de los datos. Recientemente, con el desarrollo de la Inteligencia de Negocios y Análisis de Datos, ha habido un movimiento en toda la Ciudad para proteger y asegurar los datos de una manera mejor y más regulada. No existen administradores de datos departamentales o expertos en la materia dentro de los departamentos para proporcionar orientación y requisitos a los custodios de datos de ITS. Esta necesidad es particularmente crítica cuando los Custodios de Datos están gestionando datos altamente sensibles, tales como datos probatorios u otros datos críticos de seguridad pública.

Debido a la falta de Gobernanza de Datos, las políticas y normas necesarias son inexistentes, o si existen no son adecuadas para las tareas de creación de procedimientos que garanticen una buena gestión de los sistemas de datos. El ITS de la Ciudad de Dallas ha identificado el Cuerpo Internacional de Conocimiento de Gestión de Datos (DMBOK) como un estándar de gobierno de datos y gestión de datos apropiado para su uso. Sin embargo, no existen normas para la realización de copias de seguridad y las pruebas de recuperación de datos, especialmente en el nivel de datos no estructurados. El AD 2-34 publicado para las copias de seguridad está desfasado y no representa una infraestructura moderna basada en las instalaciones y en la nube.

La Ciudad de Dallas no dispone de políticas y procedimientos adecuados de gobernanza y gestión de datos para gobernar y gestionar adecuadamente los datos de todo tipo. Además, ITS no podrá gobernar o gestionar los datos de forma apropiada o adecuada según los requisitos necesarios para la Ciudad de Dallas. Sin una gobernanza de datos adecuada y plenamente implantada, la Ciudad corre el riesgo de sufrir más pérdidas de datos, de no poder recuperarse de fallos in situ que provoquen la pérdida de datos, de tener que recuperar los datos en caso de catástrofe, de tener que asumir responsabilidades por la exposición inadecuada de los datos y de no poder aprovechar plenamente el valor analítico de los datos debido a la falta de calidad o a la incapacidad de agregarlos entre departamentos y conjuntos de datos.

La Ciudad de Dallas debe identificar un nivel apropiado y adecuado de gobernanza y gestión de datos para guiar y apoyar sus operaciones. La creación de direcciones administrativas, políticas,

procedimientos y procesos debe desarrollarse, socializarse en toda la Ciudad y seguirse adecuadamente para gobernar y proporcionar orientación. Una vez identificados, la Ciudad debe implementar, operar y gestionar las actividades de gobernanza y gestión de datos.

8 Políticas, Procedimientos, Procesos y Normas

Las políticas, los procedimientos y los procesos son componentes vitales de cualquier departamento para garantizar que las actividades y los servicios se lleven a cabo de manera oportuna. Posteriormente, rigen la gestión de los ejecutivos, los altos directivos y los empleados hacia no sólo el cumplimiento sino las mejores prácticas. Además, si los procedimientos y procesos están bien definidos, la duplicación de esfuerzos y la coherencia dentro de los procesos pueden madurarse y, a menudo, automatizarse. Las culturas anteriores habían permitido un enfoque de ejecución de los servicios de TI de "todoterreno". Esto permitía un acceso incontrolado y una gestión de los sistemas al margen de las directivas y normas administrativas.

Aunque ITS ha adoptado los controles de gestión de TI basados en las normas del NIST, hay múltiples áreas en las que el marco no se ha realizado plenamente. Las políticas, los procesos y las normas que debe seguir el personal de ITS son inadecuados. Es evidente que éstas no existen suficientemente en el equipo de copias de seguridad y almacenamiento o en la gestión de los sistemas. Los artefactos de control para la inspección de los procesos eran escasos o inexistentes. Los controles de gestión son insuficientes para proporcionar orientación y dirección al personal.

La falta de conocimientos sobre la creación, el desarrollo, el establecimiento, el funcionamiento y la gestión de políticas, procedimientos y procesos contribuyó a la pérdida de datos. Sin embargo, dadas las pruebas de que el técnico no siguió las directrices técnicas o funcionales del proveedor, la pérdida de datos no puede atribuirse únicamente a la falta de políticas, procedimientos y procesos establecidos. La falta de sistemas de control de la gestión hace que las organizaciones realicen actividades de "mejor esfuerzo" para hacer frente a las demandas y actividades diarias.

Todas las divisiones de ITS deben establecer, operar y mantener sistemas de control de gestión adecuados. Estos deben seguir un marco de mejores prácticas como el NIST. Los controles de gestión deben ser revisados y mantenidos periódicamente para comprobar su correcto funcionamiento y relevancia. Además, deben estar a disposición de la Oficina del Interventor Municipal, del Director Financiero y de la Oficina del Auditor Municipal. Posteriormente, los controles de gestión deben asignarse y documentarse a todas las actividades diarias para las operaciones de los sistemas técnicos.

9 Gestión inadecuada de los servicios informáticos

Los servicios tecnológicos deben guiarse por un proceso estandarizado. La Ciudad de Dallas adoptó ITILv3 en 2010 para la prestación de servicios a los departamentos empresariales. ITILv3 es un estándar internacional para la gestión de servicios de TI que abarca todo el sector. Los procesos de gestión de servicios identificados y descritos en ITILv3 han permitido a muchas organizaciones de servicios de TI lograr un funcionamiento cohesionado y competente, reduciendo al mismo tiempo los Costos y los riesgos para la organización. Las prácticas de gestión de servicios de tecnologías de la información (ITSM) adoptadas describen los enfoques estándar de la industria para identificar adecuadamente, el alcance, definir, diseñar, desplegar, operar y gestionar los servicios de IT para apoyar los servicios de negocio.

Los Servicios de Apoyo deben identificar y definir los servicios para su publicación en un Catálogo de Servicios Técnicos. Los servicios publicados en el Catálogo de Servicios Técnicos permitirán la identificación, el desarrollo y la publicación de los tipos de Solicitudes de Servicio apropiados que pueden ser automatizados dentro de una solución de Gestión de Servicios de IT para la supervisión y la presentación de informes de liderazgo.

ITS no opera un modelo adecuado basado en el servicio. El servicio se basa en la demanda y su aplicación es desigual para los distintos departamentos. La dirección ejecutiva de ITS debe exigir la supervisión o el cambio para garantizar que los servicios de IT tengan un alcance adecuado y funcionen en apoyo de los resultados empresariales deseados por la Ciudad y producidos por los servicios empresariales de los departamentos (por ejemplo, la inspección de edificios).

Si no se identifican, definen y operan procesos eficaces de gestión de servicios, no se establecen expectativas claras y se puede generar un "tono" organizativo inadecuado que puede llevar a ignorar los procesos y procedimientos. Los Servicios de Infraestructura de ITS no cuentan con procesos adecuados de cumplimiento de solicitudes de servicio. La falta de establecimiento de los procesos de gestión de servicios y de los procedimientos de prestación de servicios necesarios contribuyó directamente a la pérdida de datos de marzo de 2021. ITS ha iniciado un esfuerzo para madurar su proceso de gestión de servicios basado en el ITTL v3, mediante la implementación de un sistema ITSM. Sin embargo, el sistema ServiceNow es incipiente y requiere tiempo y un desarrollo adecuado del proceso para ser eficaz.

La dirección ejecutiva y la alta gerencia de ITS deben adoptar tanto la letra como el espíritu de la gestión de servicios de TI siguiendo el marco ITILv3 ya establecido. La dirección ejecutiva de ITS debe exigir que se sigan los procesos de gestión de servicios y conceder pocas o ninguna excepción de gestión. Además, la alta dirección de ITS debe actualizar periódicamente los procesos y procedimientos de gestión de servicios para que sean eficaces y eficientes en la consecución de los resultados empresariales deseados.

10 Políticas, Normas y Procedimientos de Gestión del Cambio en la Empresa

Dado que la Ciudad ha elegido adoptar ITILv3 para su marco de servicios de mejores prácticas de TI, la adhesión a esas prácticas debe realizarse plenamente. En este caso, la dirección ejecutiva de ITS no comprendió la necesidad de cumplir plenamente con las políticas, procesos y procedimientos relacionados con la gestión del cambio de la tecnología de la información de la empresa. Aunque los procesos de cambio fueron seguidos por los recursos técnicos, dichos procesos no fueron revisados o comprendidos en su totalidad para el posible efecto que condujo a la pérdida de datos. Los procesos de cambio de ITILv3 tienen ciertos criterios que deben cumplirse antes de la aprobación del cambio para seguir adelante.

Todas las funciones de los criterios no podrían haber estado correctamente en su lugar. Como se ha dicho, el marco ITILv3 establece que todo cambio debe tener un procedimiento de retirada que permita a los recursos técnicos reducir el riesgo del cambio. Si se hubiera realizado o revisado adecuadamente, el procedimiento de backout debería haber proporcionado una opción recuperable para la pérdida de los datos tras la migración. La falta de comprensión de la necesidad de cumplir plenamente con las políticas, procesos y procedimientos de gestión de cambios puso en riesgo el entorno de producción de la Ciudad, lo que condujo a la pérdida de datos. Además, durante la validación del proceso, los datos deberían haber proporcionado indicadores al técnico y a los gestores de que había problemas que podían conducir a la pérdida de datos.

La dirección de ITS no comprendió el riesgo y el impacto del cambio. Además, no se ha realizado un examen adicional del solicitante del cambio para garantizar que los cambios no puedan causar un daño grave a los datos o a la reputación de la Ciudad. Los cambios técnicos que se precipitan en el proceso con una planificación, programación, detalle y documentación deficientes no identifican todos los riesgos potenciales y son contrarios a las mejores prácticas o normas. Las prácticas de gestión de cambios aceptadas por el sector se identifican y aplican en el entorno de producción de la Ciudad. Estas prácticas de gestión del cambio identifican tipos específicos de cambio, cuándo se utilizan y los beneficios de utilizar cada tipo de cambio.

La dirección ejecutiva de ITS debe supervisar y hacer cumplir las prácticas necesarias de ITILv3, así como comunicar los elementos de alto riesgo que puedan tener un impacto negativo en el entorno de datos y la reputación de la Ciudad. Debe haber una supervisión y unas expectativas claramente definidas para el personal con el fin de generar el tono operativo adecuado en cuanto a la criticidad de la gestión del cambio de la tecnología de la información.

11 Formación Deficiente del Personal Despido y Revisión de la Capacidad

Las prácticas de Gestión Estratégica del Capital Humano dictan que una organización evalúe rutinariamente las habilidades que necesita la organización para llevar a cabo sus funciones actuales y futuras, evalúe las habilidades presentes en su fuerza de trabajo actual y desarrolle planes para desarrollar las habilidades necesarias en su fuerza de trabajo actual y/o complementar su fuerza de trabajo a través de la contratación o la subcontratación. ITS proporciona fondos para la formación de sus empleados. La organización apoya tanto las certificaciones específicas como las de rol según sea necesario para realizar las funciones del trabajo. Los proveedores de tecnología y los marcos normativos sugieren las mejores prácticas para que el personal de TI mantenga los conocimientos sobre las tecnologías que soporta el técnico. La documentación del proveedor proporciona instrucciones técnicas detalladas sobre la metodología para muchas de las acciones requeridas. La documentación técnica del proveedor proporciona precaución o componentes explícitos para instruir al técnico sobre ciertas acciones que podrían conducir a un problema perjudicial. Las instrucciones nunca se presentaron, ni se leyeron, ni fueron revisadas por los técnicos y la dirección antes de las acciones que conducían a la eliminación de datos. La dirección ejecutiva y los altos cargos de ITS no procuran ni exigen formación de forma programada para mantener los conocimientos más recientes de esas funciones. Además, la formación y la revisión por parte de la dirección no se completan. [NIST, ITILv3, Proveedor]

El técnico de almacenamiento y copias de seguridad de ITS carecía de profundidad, formación y experiencia en los procedimientos funcionales y técnicos de las mejores prácticas. Dada la asignación presupuestaria del departamento para oportunidades de formación, la dirección debería ordenar la formación técnica cuando sea apropiada para la función del puesto. Además, esto debería estar presente como un componente de la evaluación del desempeño del empleado. Las pruebas y acciones de seguimiento mantendrían las habilidades del personal y su capacidad para seguir correctamente las mejores prácticas y procesos técnicos. En este caso, un solo miembro de un equipo fue capaz de eliminar y cambiar los procedimientos definidos por el proveedor que no se ajustaban a las mejores prácticas y a los procedimientos de configuración de la solución de copia de seguridad. El personal carece de la experiencia y los conocimientos necesarios, lo que genera errores y problemas técnicos en la gestión y el almacenamiento de datos de la Ciudad.

Además, es necesario establecer la formación y la profundidad de las funciones del trabajo para varias tareas de TI, especialmente para las áreas críticas de responsabilidades. Además, deben realizarse pruebas y revisiones de esas áreas de funciones críticas. Si el equipo está compuesto por un pequeño número de personal de ITS, otros miembros del equipo funcional beneficiarían a ITS y a la Ciudad al permitir una profundidad de conocimientos para las áreas de función crítica.

City of Dallas

Sección IV- Factores Sistémicos que Rodean la Pérdida de Datos

La siguiente información describe los factores sistémicos que rodean el evento de pérdida de datos de marzo de 2021 en la Ciudad de Dallas.

12 Gestión Tono Ambiental

El tono de gestión adecuado debe establecerse mediante directivas de gestión y expectativas de rendimiento claramente documentadas. El establecimiento de este tono es necesario para que la organización tenga éxito en el cumplimiento de su misión, en este caso, la prestación de servicios de TI. El hecho de que la dirección ejecutiva y la alta gerencia de ITS no cuenten con las directivas apropiadas y las expectativas claramente documentadas provoca un colapso en la eficacia operativa. Las Normas de Control Interno en el Gobierno Federal GAO-14-704G establecen en el subcomponente 1.01 del Principio 1 que "El órgano de supervisión y la dirección deben demostrar un compromiso con la integridad y los valores éticos". El subcomponente requiere que los siguientes atributos de liderazgo "contribuyan al diseño, la implementación y la efectividad operativa de este principio":

- Tono en la cima.
- Normas de conducta.
- Adhesión a las "Normas de conducta".

La dirección ejecutiva y los altos cargos de ITS deben emplear sistemas de control de la gestión (por ejemplo, políticas, procesos, normas, procedimientos y expectativas de rendimiento), pero lo más frecuente es que las prácticas de dirección, orientación o realización de actividades se lleven a cabo mediante métodos más ad hoc, lo que provoca confusión y baja eficiencia en el personal y en la Ciudad.

Existen lagunas en las directivas de gestión documentadas y en las expectativas claras en torno a los sistemas de control de la gestión, que instancian y se comprometen con los valores fundamentales de excelencia, ética, empatía y equidad de la Ciudad de Dallas. Las técnicas de gestión de proyectos o trabajos ad hoc pueden dar lugar a incidentes como las pérdidas de datos de marzo de 2021.

La dirección ejecutiva y la alta dirección de ITS pueden crear el "tono en la cima" de la organización demostrando que la ejecución eficaz de los procesos conduce a un trabajo de calidad. Los procesos no deben ser anulados sino por la razón más excepcional.

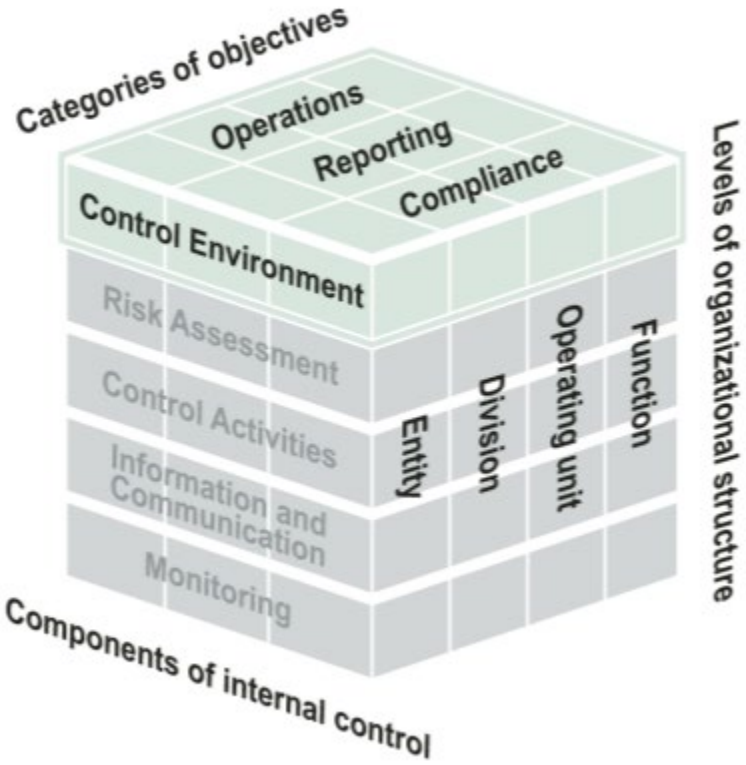


Figura 2Cubo de controles internos COSO

13 Tratamiento y Gestión de Datos, con Especial Atención a los Temas de Copia de Seguridad de Datos, Archivo de Datos y Migración de Datos

La dirección de ITS debe asegurarse de que se han implementado políticas, normas y procedimientos adecuados para el manejo de datos, a fin de garantizar que áreas como las copias de seguridad de datos, el archivo de datos y las actividades de migración de datos se realicen sobre la base de metodologías y procedimientos estándar de la industria. Por ejemplo, la norma informal es que se realicen copias de seguridad de todos los datos de producción. No existen procedimientos formales para la realización de copias de seguridad de los datos y las pruebas necesarias de las actividades de recuperación para garantizar el éxito de las actividades de copia de seguridad. No hay actividades de auditoría de los departamentos o divisiones para garantizar que se realicen las actividades de gestión de datos.

La falta de comprensión por parte del personal y la dirección de ITS de la importancia de los controles, políticas, normas y procedimientos de gestión de datos, así como de la necesaria gobernanza de estas actividades, contribuyó a la pérdida de datos de marzo de 2021. A medida que la Ciudad aumenta la cantidad de datos no estructurados que gestiona, debe asegurarse de que madura sus prácticas en torno a los datos no estructurados, como los archivos de datos perdidos en este incidente. Esa desconexión también contribuyó a que la información para los controles de datos fuera inadecuada para gestionar los datos departamentales proporcionados al grupo ITS en las funciones de custodia de datos del grupo ITS. Un problema específico es la falta de urgencia para garantizar la existencia de procedimientos adecuados de copia de seguridad y recuperación y su comprobación basada en las mejores prácticas y normas.

La Ciudad de Dallas debe implementar esfuerzos de gestión de datos estándar de la industria con una gobernanza de datos apropiada basada en un marco de gestión de datos claramente definido y aprobado. La aplicación de un marco de gestión de datos puede reducir los efectos de la manipulación inadecuada de los datos o del acceso involuntario a elementos de datos debido a un accidente o a una actividad maliciosa. Otras posibilidades de divulgación de datos regulados podrían hacer recaer sobre la Ciudad responsabilidades legales y/o financieras.

La Ciudad debe implantar un sistema de gestión de datos basado en un marco de gestión de datos estándar del sector. La gestión de datos será supervisada por un comité de gobernanza de datos que incluya a expertos en gestión de datos, expertos en análisis de datos y representantes de la empresa con conocimientos de gestión de datos, así como de las necesidades del departamento para las actividades de gestión de datos. Las pruebas de copia de seguridad y recuperación de los sistemas de datos serían una parte fundamental de la implantación de la gestión de datos. Al gestionar los datos mediante las mejores prácticas de una manera reconocida por la industria, el riesgo de pérdida de datos se reduciría en gran medida, lo que supondría un riesgo muy reducido para la Ciudad.

14 Estrategia de Contratación Inadecuada

No comprender las necesidades reales de configuración de los servicios de la solución conduce a un aprovisionamiento inexacto de los recursos que puede desviar los fondos limitados. La infradotación o sobredotación de recursos también causa problemas de gestión de recursos. Existen varias metodologías de recursos para estimar los recursos informáticos necesarios para operar un servicio de soluciones. A modo de ejemplo, la marca de servicios en la nube Microsoft Azure ofrece herramientas de estimación de uso de recursos en línea para identificar los recursos necesarios para operar un servicio de solución. ITS no utiliza adecuadamente las múltiples metodologías disponibles para estimar los recursos de tecnología de la información necesarios para operar un servicio de solución. Históricamente, ITS ha subestimado los recursos de tecnología de la información necesarios para operar un servicio de solución.

En el caso de los sucesos de pérdida de datos de marzo de 2021, la Ciudad no gestionó eficazmente los recursos e incurrió en una pérdida de datos como consecuencia de ello. ITS debe exigir la supervisión o el cambio para garantizar que la dirección y la gestión de ITS puedan informar a sus compañeros y socios comerciales de las estrategias de compra. La dirección de ITS debe aumentar la utilización de recursos técnicos imparciales y cualificados para orientar su consideración de las opciones de compra a largo plazo y las decisiones estratégicas para proporcionar recursos tecnológicos estables para el crecimiento futuro y las operaciones actuales. Las migraciones de datos y sistemas son muy arriesgadas sin una planificación estratégica y técnica. Es necesario asignar un Costo adicional a la hora de adquirir servicios de nube o de migración para garantizar que el riesgo se reduzca antes de la puesta en marcha.

Sección V- Esfuerzos de Remediación

Esta sección proporciona información relativa a los esfuerzos de corrección de la situación en la Ciudad de Dallas impulsados por los eventos de pérdida de datos de marzo de 2021.

15 Gobernanza y Gestión de Datos

ITS ha tomado las siguientes medidas para revisar, actualizar y poner en marcha un plan de gobernanza de datos que implemente una estrategia de gestión de datos para la Ciudad de Dallas:

- La Ciudad ha optado por utilizar el Marco de la Asociación de Gestión de Datos (DAMA) y el Libro de Conocimientos de DAMA versión 2 (DMBOK2) como guía principal para la implementación de la Gestión de Datos.
- Se han celebrado las primeras reuniones y revisiones con el personal ejecutivo de ITS y se ha aprobado la utilización del marco DAMA DMBOK2 como metodología para la gestión de datos de la Ciudad.
- Los esfuerzos iniciales para la gobernanza de los datos abarcan las siguientes áreas:
    - Asociarse con el Departamento de Análisis de Datos e Inteligencia Empresarial (DBI) para establecer el Consejo de Gobernanza de Datos con los miembros adecuados.
    - Identificar y establecer el Comité Directivo de Datos para crear las políticas y normas de gestión de datos adecuadas y, en su caso, los procedimientos para aplicar los requisitos promulgados por las políticas y normas.
    - Establecer un modelo de madurez de datos para la Ciudad con el fin de establecer una línea de base del nivel actual de las actividades de gestión de datos y utilizarlo como métrica para evaluar las mejoras.
    - Establecer el papel de los administradores de datos dentro de los departamentos de la Ciudad para que actúen como enlaces entre el equipo de gestión de datos y los departamentos para garantizar que se satisfacen las necesidades de datos de los departamentos mientras se trabaja dentro de un marco de mejores prácticas para la gestión de datos. Los administradores de datos deben estar centrados en el negocio, pero necesitarán un nivel de experto en la materia de los conjuntos de datos primarios de los departamentos, tanto estructurados como no estructurados.
    - Identificar la prioridad de la implementación del Área de Conocimiento de Gestión de Datos. Inicialmente las áreas de concentración son:
        - Seguridad de los datos, incluida la gestión de la privacidad y los datos regulados.

- Almacenamiento y operaciones de datos: abarca la gestión y el control de los datos estructurados, normalmente dentro de sistemas de bases de datos estructurados.
- Gestión de documentos y contenidos: abarca la gestión y el control de datos no estructurados, como imágenes, archivos almacenados en los sistemas de archivos de la Ciudad, vídeos, documentos de Word, hojas de Excel y otros. Como se ha señalado, un ejemplo sería la gestión de los datos relacionados con el evento de pérdida de datos que se está examinando.
- Calidad de los datos: esta área es fundamental para la analítica de datos y la capacidad de los datos de proporcionar valor en todo el entorno.
- Gestión de datos maestros y metadatos: inventario y documentación de los datos de la Ciudad y garantía de un uso y acceso eficaces para todas las necesidades de datos.

- Según sea necesario, proporcionar actualizaciones periódicas al personal ejecutivo sobre el estado, el progreso actual y la revisión periódica de la hoja de ruta de la gestión de datos.

16 Cambios en el Procedimiento

ITS ha tomado las siguientes medidas para actualizar los procedimientos operativos estándar y ha introducido una revisión de la gobernanza de los datos.

- Implementó un proceso de control de integridad de dos personas que requiere que varios empleados revisen y realicen las migraciones de datos.
- Se han modificado las configuraciones de los procesos de almacenamiento para exigir un periodo mínimo de 14 días antes de poder eliminar los datos de forma permanente.
- Inició una evaluación completa de los sistemas y procesos utilizados en el almacenamiento y el archivo de datos para buscar oportunidades de mejorar las capacidades y reducir el potencial de pérdida de datos.
- Se ha actualizado el Plan de Respuesta a Incidentes y Preparación para la Violación de Datos para incluir la notificación al Alcalde y al Concejo de la Ciudad sobre cualquier compromiso de datos dentro de las dos horas siguientes a la notificación al Equipo de Liderazgo Ejecutivo de la Ciudad.

17 Esfuerzos de Recuperación de Datos

ITS Risk/Compliance ha tomado las siguientes medidas:

- Buscar en los sistemas de la Ciudad cualquier resto de los datos perdidos.
- Comenzó con la lista original proporcionada por el Grupo de Servidores.
- Se ha movido a la lista de información analizada.
- Lista inicial proporcionada por el Departamento de Policía de Dallas.
- Trabajar con la lista actual de prioridades del Fiscal del Distrito.
- Búsqueda en el entorno de Microsoft Office 365, incluidas las ubicaciones de correo electrónico, SharePoint y OneDrive.
- Escribir un script para buscar en sistemas basados en el número de caso/nombre del detective/términos de búsqueda.
- Se ha añadido un consultor externo al equipo que está proporcionando dirección y recursos adicionales.

Entorno de recuperación

Se ha construido un entorno de recuperación para apoyar los esfuerzos de recuperación actuales y futuros. Se ha empezado a trabajar para reconstruir el Servidor de Fusión y los conjuntos de datos a partir de las imágenes forenses de la copia BIT. El entorno de recuperación permite a ITS restaurar conjuntos de datos desde puntos históricos en el tiempo. Una vez que los datos han sido restaurados, pueden ser validados. Una vez validados los datos, se pueden realizar búsquedas y, si el conjunto de datos contiene datos que faltan, los datos se pueden restaurar de nuevo en los servidores de producción. El entorno de recuperación se utilizará para probar varios procedimientos de copia de seguridad y recuperación para cualquier servidor o sistema de nuestro entorno que esté siendo respaldado por Commvault. Estos procedimientos incluyen la restauración de conjuntos de datos a partir de los siguientes tipos de copias de seguridad:

- Copias de seguridad completas: Realiza una copia de seguridad de toda la máquina virtual. Esta es la copia de seguridad más completa.
- Copias de seguridad incrementales: Realiza copias de seguridad de los datos de la máquina virtual que han cambiado desde la última copia de seguridad.

- Copias de seguridad completas sintéticas: Consolida los datos de la máquina virtual de la copia de seguridad completa más reciente con las copias de seguridad incrementales posteriores.

Imagen forense del servidor de fusión y de los datos

Se ha tomado una imagen forense del servidor FUSION del Departamento de Policía de Dallas y de su disco de datos de 14,5 TB. Esta imagen de copia BIT conservará el servidor y los datos a partir del sábado 11 de septiembre. Las unidades se han recuperado del centro de datos del DPD y se han instalado en el Ayuntamiento, donde se están realizando varias copias. Una será una copia Dorada que se conservará, una copia opcional en la Nube para ser cargada en Azure, y una Copia de Trabajo que se convertirá en una Imagen para ser utilizada por VMware o Azure para nuestro proyecto de "Entorno de Recuperación" y "Búsqueda de Datos".

Búsqueda de contenidos

Se ha comenzado a trabajar para perfeccionar nuestros esfuerzos de "Búsqueda de contenidos en O365". Se han creado dos unidades compartidas y se ha concedido acceso al "Equipo de Búsqueda". Los archivos de trabajo, que son "hojas de cálculo" con los datos de los casos que faltan, se han perfeccionado y cargado en el servidor de recuperación de datos. ITS ha comenzado a perfeccionar el proceso de recopilación y búsqueda de datos para aumentar la velocidad y ampliar nuestros esfuerzos. Hasta ahora, todos los esfuerzos han sido realizados por el equipo de eDiscovery. El plan consiste en utilizar recursos contratados para buscar los datos según criterios de casos específicos y consolidar los resultados en "cadenas de búsqueda" que puedan introducirse fácilmente en el 0365 Compliance Search. En la actualidad, se tarda hasta una hora o más en reunir la información e introducirla en la herramienta de búsqueda. También hemos ampliado nuestros esfuerzos de búsqueda en Office 365, incluyendo los buzones de Exchange Online, OneDrive y las ubicaciones de SharePoint.

Servidor de búsqueda seguro

Actualmente estamos construyendo un sistema que perfeccionará y nos permitirá ampliar nuestros esfuerzos de búsqueda de contenidos. Además de los esfuerzos de los equipos de eDiscovery, hemos añadido recursos adicionales, incluyendo 4 contratistas de tecnología para buscar en los buzones de correo de Exchange Online, OneDrive y SharePoint cuando se trate de ubicaciones de datos archivados y huérfanos perdidos. En este momento, nuestro equipo de servidores ha construido un servidor de

búsqueda segura de desarrollo/prueba. Este servidor incluye SQL y una aplicación web frontal personalizada que se utiliza para buscar grandes archivos de datos para varios campos, incluyendo pero no limitado a: Número de Caso, Nombre del Caso, Número de Placa, Nombre del Oficial y nombres de archivos en cuestión. Los datos se utilizan entonces para formular búsquedas de contenido por parte de nuestro equipo de eDiscovery y de los contratistas. A continuación, los datos se empaquetan en archivos .pst para que el DPD los utilice para completar los datos de los casos que faltan.

Actualmente se está construyendo un servidor de producción que albergará permanentemente la aplicación de búsqueda segura, el sitio web y la correspondiente base de datos SQL. Este servidor permitirá la importación de nuevos conjuntos de datos y dará tanto a ITS como al equipo de eDiscovery y a DPD la capacidad de buscar rápidamente datos relacionales y exportar los resultados. Este servidor está diseñado específicamente para ser utilizado por recursos no técnicos para realizar rápidamente complejas búsquedas de datos basadas en SQL.

Detección y respuesta de puntos finales (EDR)

Los contratistas del equipo de búsqueda de contenidos han asistido a una formación sobre la herramienta de búsqueda EDR. Como parte de la detección de virus y amenazas, el EDR indexa todos los archivos de todos los ordenadores y servidores. Esto nos permite buscar nombres de archivos específicos en todos los puntos finales conectados en todas las ubicaciones. Esta herramienta es el último recurso para buscar en todos los puntos finales de la red, incluidos los servidores y las estaciones de trabajo de los usuarios. El equipo tiene acceso a la consola y permisos de búsqueda. Cuando un caso de "búsqueda" se eleva a un punto en el que los métodos normales de búsqueda de contenido son improductivos, la Búsqueda EDR será el último recurso. La herramienta es muy específica en cuanto a los criterios de búsqueda, por lo que es mejor utilizarla para archivos específicos por su nombre.

Búsqueda global de Commvault

ITS está utilizando la barra de búsqueda global en el Centro de Comando para ayudar en los esfuerzos de recuperación de datos. En los entornos de CommCell en los que todos los servidores de índice están en la nube o en local, puede utilizar la barra de búsqueda global para buscar, añadir y realizar acciones en entidades (como servidores de archivos, hipervisores y usuarios) y elementos de navegación (como ordenadores portátiles). En las búsquedas, puede utilizar el lenguaje natural. Si tiene varios entornos de

servicio CommCell en un entorno CommCell, las búsquedas globales incluyen todos los entornos CommCell.

Por ejemplo, desde la barra de búsqueda global se puede hacer lo siguiente Buscar y eliminar un usuario, Ir a un servidor de archivos, Hacer una copia de seguridad o restaurar una aplicación en la nube, Añadir un servidor y Buscar archivos.

ITS Risk/Compliance ha tomado las siguientes medidas:

- Búsqueda en los sistemas de la Ciudad de cualquier resto de los datos perdidos Comenzó con la lista original proporcionada por Server Group Pasó a la lista de información analizada Lista inicial proporcionada por el Departamento de Policía de Dallas Trabajo con la lista actual de las prioridades del Fiscal de Distrito Búsqueda de correos electrónicos.
- Escritura de un script para buscar en los sistemas basado en el número de caso/nombre del detective/términos de búsqueda Se ha añadido un especialista externo al equipo que puede proporcionar recursos adicionales Imagen forense del servidor de fusión y de los datos.
- Se ha tomado una imagen forense del servidor FUSION del Departamento de Policía de Dallas y de su disco de datos de 14,5 TB. Esta imagen de copia BIT preservará el servidor y los datos a partir del sábado 11 de septiembre. Las unidades se recuperarán del centro de datos del DPD y se instalarán en el Ayuntamiento, donde se harán varias copias. Una copia Dorada que se conservará, una copia opcional en la Nube para ser cargada en Azure, y una Copia de Trabajo que se convertirá en una Imagen para ser utilizada por VMware o Azure para nuestro proyecto de "Entorno de Recuperación" y "Búsqueda de Datos".
- Búsqueda de contenidos Se ha comenzado a trabajar para perfeccionar nuestros esfuerzos de "Búsqueda de contenidos en O365". Se han creado dos unidades compartidas y se ha concedido acceso al "Equipo de Búsqueda". Se han perfeccionado los archivos de trabajo "Spread sheets" con los datos de los casos perdidos y se han cargado en el servidor de recuperación de datos.
- Hemos empezado a perfeccionar el proceso de recopilación y búsqueda de datos para aumentar la velocidad y ampliar nuestros esfuerzos. Hasta ahora, todos los esfuerzos han recaído en el equipo de eDiscovery. El plan consiste en utilizar recursos contratados para buscar los datos en función de criterios de casos específicos y consolidar los resultados en "cadenas de búsqueda" que puedan introducirse fácilmente en el 0365 Compliance Search. En la actualidad, se tarda

hasta una hora o más en reunir la información e introducirla en la herramienta de búsqueda. También tenemos previsto ampliar nuestros esfuerzos de búsqueda a OneDrive y SharePoint cuando sea posible.

- Los contratistas de EDR han asistido a la formación programada para la herramienta de búsqueda de EDR. Esta herramienta es el último recurso para buscar en todos los puntos finales de la red, tanto en los servidores como en las estaciones de trabajo de los usuarios. El equipo tiene acceso a la consola y permisos de búsqueda. Cuando un caso de "búsqueda" se eleva a un punto en el que los métodos normales de búsqueda de contenido son improductivos, la búsqueda EDR será el último recurso. La herramienta es muy específica en cuanto a los criterios de búsqueda, por lo que es mejor utilizarla para archivos específicos por su nombre.

City of Dallas

Sección VII- Recomendaciones

Esta sección esboza las recomendaciones generales que se cree que ofrecen un valor potencial a los procesos, procedimientos y actividades de gobierno y gestión de datos en la Ciudad de Dallas. ITS ofrece estas recomendaciones generales debido a la autorreflexión disponible realizada dentro del departamento.

18 Recomendación 1 - Gobernanza y Gestión de Datos

Se recomienda que ITS establezca un programa de gestión de datos para la creación y gestión de una gobernanza de datos adecuada para la Ciudad de Dallas. La gestión de datos puede aumentar la visibilidad, fiabilidad, escalabilidad, integridad y disponibilidad de los datos en toda la empresa. La máxima prioridad es la disponibilidad y fiabilidad de los datos. Si los datos no están disponibles, no tienen valor. Si los datos no son fiables, tienen poco valor. Otras áreas, como la seguridad de los datos, la calidad de los datos o la gestión de los metadatos, se basan en la disponibilidad y la fiabilidad de los datos.

Un sistema de gestión de datos correctamente implantado a nivel de empresa con un sistema de gobernanza propio y gestionado en un formato centralizado proporciona la estructura y el marco para aplicar políticas y normas de datos en toda la empresa. El equipo de gobernanza proporciona dirección para la gestión de datos a la dirección de la Ciudad. Basándose en el AD 2-25, los departamentos deberían asignar administradores de datos para entender y ayudar en la gestión de los mismos.

El Departamento de ITS debería tomar las siguientes medidas:

1. Establecer un grupo de gestión de datos para iniciar una estrategia de gestión de datos a nivel de empresa implementada por un comité de gobernanza de datos (dirigido por el DBI) y un grupo de dirección de datos para supervisar el proceso.
2. Identificar las metas y objetivos empresariales para garantizar que la gestión de datos esté en consonancia con los departamentos de la Ciudad.
3. Identificar las áreas prioritarias, como la falta de gestión del contenido de los datos no estructurados, que fue un factor instigador de la pérdida de datos.
4. Crear una hoja de ruta con un calendario provisional para la aplicación de las distintas áreas y procesos del marco de gestión de datos.
5. Diseñar e instituir una función de administrador de datos dentro de la Ciudad a nivel de departamento. El administrador de datos debe ser un experto en la materia dentro del departamento, así como en los datos creados dentro del departamento. El gestor de datos actuará como enlace entre el equipo de gestión de datos y el departamento para garantizar que las políticas y normas requeridas se entregan al departamento, y que el departamento

instituye procedimientos para garantizar el cumplimiento de dichas políticas y procedimientos.

6. Instituir análisis y métricas para medir y seguir la madurez de la gobernanza y la gestión de datos.

19 Recomendación 2 - Cambios de Procedimiento Inmediatos

ITS debería tomar las siguientes medidas para actualizar los procedimientos operativos estándar y los procesos.

1. ITS debería colaborar con el proveedor para revisar y actualizar los procedimientos de copia de seguridad, recuperación, archivo, eliminación, etc., para que coincidan con el rendimiento óptimo del proveedor.
2. Búsqueda continua y realización de los cambios técnicos necesarios en los sistemas de la Ciudad para los restos de datos perdidos.
3. Implementó un proceso de control de integridad de dos personas que requiere que varios empleados revisen y realicen las migraciones de datos.
4. Cambiar las configuraciones en los procesos de almacenamiento para exigir un período mínimo de 14 días antes de que los datos puedan ser eliminados permanentemente.
5. Iniciar una evaluación de arriba abajo de los sistemas y procesos utilizados en el almacenamiento y archivo de datos para buscar oportunidades de mejorar las capacidades y reducir el potencial de pérdida de datos.
6. Actualizar el Plan de Respuesta a Incidentes y Preparación para la Violación de Datos para incluir la notificación al Alcalde y al Concejo de la Ciudad sobre cualquier compromiso de datos dentro de las dos horas siguientes a la notificación al Equipo de Liderazgo Ejecutivo de la Ciudad.
7. Implantar/validar la nueva regla 3-2-2 de copia de seguridad de BC/DR:
    a. Guarde 3 copias de sus datos.
    b. Almacenar 2 copias de seguridad localmente pero en diferentes dispositivos.
    c. Almacenar 2 copias fuera del sitio (1 copia en una ubicación remota + 1 copia en la nube).
8. Siga los procedimientos de gestión de cambios para garantizar una recuperación adecuada.
9. Ofrecer oportunidades de formación continua para mejorar el rendimiento.
10. ITS Risk/Compliance debe realizar una revisión anual de los cambios realizados en las políticas y procedimientos.

20 Recomendación 3 - Documentación de Requisitos y Procesos de Evaluación de Riesgos

Se recomienda que la dirección de ITS:

1. La dirección ejecutiva y la alta gerencia de los ITS deben comprender la necesidad de documentar los procesos y de realizar una evaluación exhaustiva de los riesgos, especialmente en el caso de las actividades poco frecuentes y de alto riesgo. ITILv3 proporciona categorías y dirección para la documentación.
2. La dirección ejecutiva y la alta gerencia de ITS deben establecer el tono ambiental apropiado de que las acciones tienen repercusiones y que se deben tomar las actividades de mitigación de riesgos apropiadas para asegurar que se logren los resultados empresariales deseados.
3. La dirección ejecutiva y la alta gerencia de los ITS deben realizar una supervisión exhaustiva de la evaluación de riesgos para garantizar que se realicen las actividades apropiadas y adecuadas de forma que se reduzcan los riesgos.
4. La dirección ejecutiva de ITS debe incluir el cumplimiento de las normas reglamentarias y contractuales antes de que una solución pueda solicitar su traslado al entorno de producción de la Ciudad.

21 Recomendación 4 - Gestión de Cuentas y Accesos

Se recomienda que la dirección de ITS:

1. La dirección ejecutiva y la alta gerencia de ITS deberían tomar ciertas medidas organizativas para evitar futuras pérdidas de datos de este tipo.
2. El liderazgo debe inculcar un sentido de integridad a través de un tono organizativo adecuado.
3. La dirección ejecutiva y la alta gerencia de ITS deben detener los despliegues en caso de fallo del script de despliegue y comenzar la ejecución de los planes de retirada.
4. Todas las actividades realizadas bajo un administrador deben ser rastreadas y asignadas a la cuenta administrativa.
5. El personal de la Ciudad no debe utilizar las cuentas de administrador para operar los servicios como ocurrió en este caso.

22 Recomendación 5 - Procesos de Contratación y Gestión de Proveedores

El personal de ITS debe tener las habilidades suficientes para abordar los problemas de conflicto entre el proveedor y la Ciudad, con una comprensión completa de los sistemas. En última instancia, ITS es responsable de los sistemas gestionados por los proveedores y debe garantizar que los procesos y procedimientos se ajusten a esa responsabilidad del proveedor.

Se recomienda que la dirección de ITS:

1. El ejecutivo y la alta dirección de ITS deben haber identificado el alcance y los requisitos incluidos en las negociaciones contractuales antes de la implementación de los servicios.
2. La gestión de los contratos debe obligar a los proveedores a cumplir unos parámetros de rendimiento medibles.

23 Recomendación 6 - Gestión Innovadora de los Datos del DPD

El Departamento de Policía de Dallas se beneficiaría de la implantación de un sistema de gestión de datos en toda la Ciudad de Dallas. La recomendación es un sistema de gestión de datos centralizado con un grupo de gobernanza de datos que diseñe y supervise la implementación de la gestión de datos. Esto garantiza un conjunto único de políticas y normas en toda la Ciudad con la flexibilidad necesaria para que cada departamento aplique procedimientos basados en las necesidades y requisitos específicos del departamento.

Algunos ejemplos de necesidades específicas dentro del DPD para la gestión de datos serían:

1. La creación de uno o varios gestores de datos dentro del DPD. Cada administrador de datos sería un experto en los datos utilizados en el DPD y en las aplicaciones que los utilizan. El administrador de datos se encargaría de coordinar con el equipo de gestión de datos de ITS la aplicación de las políticas y normas de datos de toda la Ciudad.
2. El (los) administrador(es) de datos del DPD sería(n), por ejemplo, responsable(s) de garantizar el cumplimiento de los requisitos basados en las direcciones administrativas existentes o creadas. El documento AD 2-25 establece que el director de cada departamento es el propietario de los datos creados principalmente en el departamento. El administrador de datos será probablemente el agente en funciones del propietario de los datos en la mayoría de los departamentos. El propietario de los datos es responsable de la clasificación de los datos dentro del departamento en función de las especificaciones del AD. Una vez clasificados, el propietario/administrador de datos es responsable de trabajar con los custodios de datos (normalmente ITS) para garantizar que los datos se gestionan en función de los requisitos de clasificación.
3. Existirían políticas y normas para todos los ámbitos de la gestión de datos, de modo que cada departamento, incluido el DPD, tendría una clara comprensión y delimitación de las funciones y responsabilidades en cada ámbito de los datos.
4. Se realizarán auditorías periódicas para garantizar que los datos se gestionan de acuerdo con los procedimientos del departamento. Por ejemplo, si los datos se clasifican como sensibles, como los datos probatorios, los procedimientos deben estar claramente definidos para el

almacenamiento, las copias de seguridad, las pruebas de recuperación, la recuperación de desastres y la gestión de cambios para los datos.

24 Recomendación 7 - Políticas, Procedimientos, Procesos y Normas

Las políticas, los procedimientos y los procesos son componentes vitales de cualquier departamento para garantizar que las actividades y los servicios se lleven a cabo de manera oportuna.

Se recomienda que la dirección de ITS:

1. Todas las divisiones de ITS deben establecer, operar y mantener sistemas de control de gestión adecuados. Estos deben seguir un marco de mejores prácticas como el del NIST.
2. Los controles de gestión deben ser revisados y mantenidos periódicamente para comprobar su correcto funcionamiento y relevancia. Además, deben estar a disposición de la Oficina del Interventor Municipal, del Director Financiero y de la Oficina del Auditor Municipal.
3. Los controles de gestión deben asignarse y documentarse a todas las actividades diarias para las operaciones de los sistemas técnicos.

25 Recomendación 8 - Gestión Inadecuada de los Servicios de TI

Los procesos de gestión de servicios identificados y descritos en ITILv3 han permitido a muchas organizaciones de servicios de TI lograr un funcionamiento cohesionado y competente, reduciendo al mismo tiempo los Costos y los riesgos para la organización.

Se recomienda que la dirección de ITS:

1. La dirección ejecutiva y la alta gerencia de ITS deben adoptar tanto la letra como el espíritu de la gestión de servicios de TI siguiendo el marco ITILv3 ya establecido.
2. La dirección ejecutiva de ITS debe exigir que se sigan los procesos de gestión de servicios y conceder pocas excepciones de gestión, si es que las hay.
3. La alta dirección de ITS debe actualizar periódicamente los procesos y procedimientos de gestión de servicios para que sean eficaces y eficientes en la consecución de los resultados empresariales deseados.

26 Recomendación 9 - Políticas, Normas y Procedimientos de Gestión del Cambio en la Empresa

Los procesos de cambio de ITILv3 tienen ciertos criterios que deben cumplirse antes de la aprobación del cambio para seguir adelante.

Se recomienda que la dirección de ITS:

1. La dirección ejecutiva de ITS debe supervisar y aplicar las prácticas ITILv3 necesarias, así como comunicar los elementos de alto riesgo que puedan tener un impacto negativo en el entorno de datos y la reputación de la Ciudad.
2. Debe haber una supervisión y unas expectativas claras para el personal a fin de engendrar el tono operativo adecuado en cuanto a la criticidad de la gestión del cambio de la tecnología de la información.

27 Recomendación 10 - Formación Deficiente del Personal, Despido y Revisión de la Capacidad

Las prácticas de Gestión Estratégica del Capital Humano dictan que una organización evalúe rutinariamente las habilidades que necesita la organización para realizar sus funciones actuales y futuras, evalúe las habilidades presentes en su fuerza de trabajo actual y desarrolle planes para desarrollar las habilidades necesarias en su fuerza de trabajo actual y/o complementar su fuerza de trabajo a través de la contratación o la subcontratación.

Se recomienda que la dirección de ITS:

1. Además, es necesario establecer la formación y la profundidad de las funciones del trabajo para varias tareas de TI, especialmente para las áreas críticas de responsabilidades. Además, deben completarse las pruebas y la revisión de esas áreas de funciones críticas.

2. La formación debería ser obligatoria para varios miembros de un equipo, incluida la formación ofrecida fuera de los entornos tradicionales. Si el equipo está compuesto por un número reducido de personal de ITS, otros miembros del equipo funcional beneficiarían a ITS y a la Ciudad al permitir profundizar en el conocimiento de las áreas de función crítica.

28 Recomendación 11 - Tono Ambiental de la Gestión

El tono de gestión adecuado debe establecerse mediante directivas de gestión y expectativas de rendimiento claramente documentadas. Es necesario establecer este tono para que la organización tenga éxito en el cumplimiento de su misión, en este caso, la prestación de servicios de TI.

Se recomienda que la dirección de TI:

1. La dirección ejecutiva y los altos cargos de los ITS deben emplear de forma apropiada y adecuada los sistemas de control de la gestión (por ejemplo, políticas, procesos, normas, procedimientos y expectativas de rendimiento).

2. Subsanar las deficiencias en las directivas de gestión documentadas y las expectativas en torno a los sistemas de control de la gestión. Estos sistemas deben enfatizar el compromiso necesario con los valores fundamentales de la Ciudad de Dallas: excelencia, ética, empatía y equidad. Las técnicas de gestión de proyectos o trabajos ad hoc pueden provocar incidentes como los de la pérdida de datos de marzo de 2021 y deben eliminarse.

3. La dirección ejecutiva y la alta gerencia de ITS deben crear el necesario "tono en la cima" de la organización, demostrando que la ejecución eficaz de los procesos conduce a un trabajo de calidad. Los procesos no deben ser anulados sino por la razón más excepcional.

29 Recomendación 12 - Manejo y Gestión de Datos con un Enfoque Específico en el Tema de la Copia de Seguridad de Datos, el Archivo de Datos y la Migración de Datos

A medida que la Ciudad aumenta la cantidad de datos no estructurados que gestiona, debe asegurarse de que madura sus prácticas en torno a los datos no estructurados

Se recomienda que la dirección de TI:

1. La Ciudad debe implantar un sistema de gestión de datos basado en un marco de gestión de datos estándar del sector.

2. La gestión de datos sería supervisada por un comité de gobernanza de datos que incluiría a expertos en gestión de datos, expertos en análisis de datos y representantes de la empresa con conocimientos de gestión de datos, así como de las necesidades del departamento para las actividades de gestión de datos.

3. Las pruebas de copia de seguridad y recuperación de los sistemas de datos serían una parte fundamental de la implantación de la gestión de datos. Al gestionar los datos mediante una práctica recomendada de forma reconocida por el sector, el riesgo de pérdida de datos se habría reducido en gran medida, lo que supondría un riesgo casi nulo para la Ciudad.

City of Dallas

30 Recomendación 13 - Estrategia de Contratación Inadecuada

Existen varias metodologías de recursos para estimar los recursos informáticos necesarios para operar un servicio de soluciones.

Se recomienda que la dirección de TI:

1. En el caso de los sucesos de pérdida de datos de marzo de 2021, la Ciudad no gestionó eficazmente los recursos e incurrió en una pérdida de datos como consecuencia de ello. ITS debe exigir la supervisión o el cambio para garantizar que la dirección y la gestión de ITS puedan informar a sus compañeros y socios comerciales de las estrategias de compra.

2. La dirección de ITS debe considerar las opciones de compra a largo plazo y las decisiones estratégicas para proporcionar recursos tecnológicos estables para el crecimiento futuro y las operaciones actuales.

3. Las migraciones de datos y sistemas son muy arriesgadas sin una planificación estratégica y técnica. Es necesario asignar un Costo adicional cuando se adquieren servicios de nube o de migración para garantizar que el riesgo se reduce antes de la puesta en marcha.

City of Dallas

Sección VI- Directrices Administrativas de la Ciudad de Dallas

A continuación se describe qué son las Directivas Administrativas de la Ciudad de Dallas y las Directivas Administrativas pertinentes para los servicios de información y tecnología.

31 Directivas Administrativas de la Ciudad de Dallas

Una directiva administrativa es un documento autorizado y emitido por el Administrador de la Ciudad para establecer prácticas y procedimientos operativos para determinadas funciones administrativas y/o para complementar la dirección política más amplia del Concejo de la Ciudad aumentando/aclarando ordenanzas y enmiendas al Código de la Ciudad o a las políticas y procedimientos de personal de la Ciudad. Las direcciones administrativas se centran generalmente en las políticas y prácticas internas y están diseñadas para promover prácticas empresariales coherentes, mejorar la comunicación organizativa, reducir el riesgo y la exposición, y proporcionar los controles internos necesarios sobre los recursos y las transacciones comerciales. [Marana]

Las direcciones administrativas de la Ciudad de Dallas pueden pertenecer actualmente a una de las siguientes categorías:

- Organización
- General
- Personal
- Finanzas y Compras
- Asuntos legales
- Propiedad

Una dirección administrativa puede iniciarse y desarrollarse a nivel de departamento. El departamento que la inicie identificará a los principales interesados y los incluirá en el desarrollo de la directiva. Se espera que ciertos departamentos sean identificados como partes interesadas clave dependiendo del tema, para incluir (pero no limitado a): [Marana]

- Empleados
- Fondos/monedas
- Tecnología
- Instalaciones
- Registros
- Comunicación
- Ciudadanos/empresas/servicio al cliente

- Legislación
- Activos (por ejemplo, equipos y vehículos)
- Planificación/operación/gestión de emergencias
- Ley
- Seguridad

Todos los proyectos de las direcciones administrativas se someterán al proceso de elaboración y publicación descrito en la Dirección Administrativa 2-01 (AD 2-01) Directivas Administrativas.

Todas las direcciones administrativas deben ser aprobadas y emitidas oficialmente por el Administrador de la Ciudad.

Todos los empleados son responsables de leer, comprender y hacer preguntas para aclarar las direcciones administrativas. El incumplimiento de una dirección administrativa puede ser motivo de acción disciplinaria. [Marana]

31.1 AD 2-XX - Gobernanza y Gestión de Datos (en desarrollo)

ITS está elaborando una Dirección Administrativa para crear un programa más sólido de Gobernanza y Gestión de Datos.

31.2 AD 2-24- Seguridad Informática

La Dirección Administrativa 2-24 (AD 2-24) Seguridad Informática establece las normas y procedimientos que rigen la seguridad de los sistemas y activos de información de la Ciudad. El propósito del AD 2-24 es también proteger y preservar la confidencialidad, integridad, disponibilidad, responsabilidad y garantía de los sistemas y activos de información. El AD 2-24 tiene un amplio alcance, ya que se aplica a todos los departamentos, personas y dispositivos que conforman los sistemas y activos informáticos de la Ciudad. [AD 2-24]

El AD 2-24 define diferentes responsabilidades para las distintas partes de la organización. El AD 2-24 exige que los Departamentos de la Ciudad se adhieran a las Normas de Seguridad Empresarial del Departamento de Servicios de Información y Tecnología. [AD 2-24]

Además, los Departamentos de la Ciudad están obligados a tomar medidas razonables para proteger los activos, recursos y datos de TI de la Ciudad contra el acceso, uso, divulgación, modificación y destrucción no autorizados con el fin de proporcionar integridad, confidencialidad y disponibilidad en la utilización de los recursos de información para prestar servicios a las partes interesadas de la Ciudad. [AD 2-24]

El AD 2-24 también establece los requisitos para el Director de Información. Según el AD 2-24, el Director de Información debe recomendar la visión estratégica, las políticas, las orientaciones y proporcionar otros consejos relacionados con la tecnología de la información al Administrador de la Ciudad. [AD 2-24]

El Director de Información también es responsable de aplicar políticas, normas, herramientas y recursos de seguridad de la información eficaces y adecuados para proteger los sistemas de información de la Ciudad y reducir los riesgos inherentes al funcionamiento de los sistemas de almacenamiento de datos y prestación de servicios. [AD 2-24]

El AD 2-24 también establece requisitos para los empleados de la Ciudad. Los empleados de la Ciudad deben cumplir con el AD 2-24, así como con otras políticas que rigen el comportamiento, las actividades, la conducta, el desempeño y el uso aceptable de los sistemas y activos de información. El AD 2-24 establece los mismos requisitos para los proveedores que interactúan con los sistemas y activos de información de la Ciudad. [AD 2-24]

La norma AD 2-24 está vinculada a otras normas del sector de las TI que tratan de la seguridad informática. Como tal, el AD 2-24 establece el uso de marcos y normas de seguridad reconocidos por la industria, incluidos los del Instituto Nacional de Ciencia y Tecnología y las Normas Federales de Publicación de Información (resultantes de la aprobación de la Ley Federal de Gestión de la Seguridad de la Información de 2002). [AD 2-24]

Además, el AD 2-24 hace que la división de Seguridad de los ITS sea la única responsable de la planificación, el diseño, el desarrollo, la implementación y la gobernanza de la arquitectura de seguridad que protege las redes de la Ciudad y permite al personal aprovechar los recursos de información para garantizar servicios eficaces. [AD 2-24]

El AD 2-24 continúa definiendo la protección de la privacidad, la gestión general de los datos y la gestión de la respuesta a incidentes. Aunque se discuten varios temas, el AD 2-24 proporciona una orientación

de alto nivel que establece las responsabilidades y expectativas de cada parte que trata con los recursos de información en el curso de la realización de negocios en nombre de la Ciudad de Dallas. [AD 2-24]

31.3 AD 2-25 - Propiedad y Clasificación de los Datos

La Dirección Administrativa 2-25 (AD 2-25) Clasificación y Propiedad de Datos establece clasificaciones para los datos basadas en la confidencialidad o la importancia de los mismos. [AD 2-25]

El AD 2-25 se aplica a todos los datos recogidos y mantenidos por la Ciudad de Dallas. Esto incluye los datos que residen en todos los ordenadores de la Ciudad (microordenadores, redes de área local, redes de área amplia, sistemas de teleproceso, sistema operativo, terminales digitales móviles, servicios en línea, conexiones a Internet). Sin embargo, la lista del AD 2-25 no pretende ser exhaustiva. [AD 2-25]

El AD 2-25 define diferentes responsabilidades en torno a los datos. El AD 2-25 encarga al Departamento de Servicios de Información y Tecnología la custodia física de los datos. En este papel, el Departamento (y específicamente el Equipo de Seguridad) es responsable de proporcionar una lista de archivos de datos del mainframe y de la red corporativa a los departamentos, también conocidos como Propietarios de Datos, para los cuales el Departamento de Servicios de Información y Tecnología es el Custodio Físico de los datos. [AD 2-25]

Para los propietarios de datos, el AD 2-25 establece que los propietarios de datos son responsables de garantizar que todos los datos recopilados por ellos o para su uso estén debidamente clasificados. Los propietarios de los datos también son responsables de revisar todos los archivos de datos de forma periódica para garantizar que cada archivo de datos está correctamente clasificado y que sólo los usuarios necesarios pueden acceder a esos datos en los sistemas informáticos de la Ciudad de Dallas. [AD 2-25]

El AD 2-25 define los niveles de clasificación de datos de la siguiente manera:

1. Confidencial: es una excepción obligatoria o permisiva a la divulgación según la Ley de Registros Abiertos de Texas. El acceso, a cualquier nivel, debe ser aprobado por el propietario de los datos.

2. Producción - Datos no confidenciales, pero que también se consideran críticos por su importancia para la organización y su funcionamiento. El acceso a las actualizaciones está restringido y debe ser aprobado por el propietario de los datos.
3. Prueba - Datos ni confidenciales, ni de producción. Los datos de prueba pueden ser leídos por cualquier persona y pueden ser actualizados por el departamento o grupo de trabajo que los creó (propietario de los datos). El acceso a las actualizaciones requiere la aprobación del propietario de los datos. [AD 2-25]

El AD 2-25 asigna específicamente el papel singular de Propietario de Datos al Director del departamento que solicitó o autorizó la creación de los datos. Sin embargo, el Director del departamento también puede delegar la autoridad para aprobar las solicitudes de acceso, pero mantendrá la responsabilidad de garantizar que los datos estén protegidos de acuerdo con las leyes federales, estatales y locales. Los propietarios de los datos también están obligados a examinar todos sus datos, basándose en las clasificaciones definidas en la Dirección Administrativa. [AD 2-25]

El Departamento de Servicios de Información y Tecnología también está obligado por el AD 2-25 a preparar una lista anual de los archivos de datos bajo su custodia, con sus clasificaciones. Los propietarios de los datos deben revisar la lista y aceptar la propiedad de sus archivos de datos en un plazo de dos semanas tras recibir la lista. [AD 2-25]

El AD 2-25 también exige a todos los propietarios de datos que formen a su personal en el manejo adecuado de los datos confidenciales. Esta formación debe incluir la identificación de los datos designados como confidenciales, la exhibición de los datos confidenciales en áreas con tráfico público y la forma en que deben tratarse las solicitudes de acceso a los datos confidenciales, ya sea de otras entidades de la Ciudad o del público. [AD 2-25]

El documento AD 2-25 está siendo revisado para actualizarlo e incluirá lo siguiente:

- Clasificación adicional de los datos de la normativa. Esta clasificación se utiliza para identificar los datos sujetos a procedimientos de tratamiento específicos, como los de los Sistemas de Información de Justicia Penal (CJIS) y la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA).

- Posible inclusión de una clasificación de datos de carácter probatorio. Esta clasificación se referiría a datos como los que posee el Departamento de Policía de Dallas. Esta clasificación requerirá que el propietario de los datos proporcione métodos documentados sobre cómo deben manejarse, respaldarse y conservarse dichos datos con fines probatorios.
- El término Archivo de Datos debe entenderse como la inclusión de tipos de archivos adicionales más allá de los archivos planos mantenidos para apoyar las operaciones anteriores del mainframe.

31.4 AD 2-28 - Gestión del Cambio de la Tecnología de la Información

La Dirección Administrativa 2-28 (AD 2-28) Gestión del Cambio de la Tecnología de la Información existe para garantizar que se mantengan entornos operativos de tecnología de la información estables y que todos los cambios en los sistemas informáticos tengan directrices, normas y procedimientos documentados para planificar, coordinar, supervisar y recuperar los cambios en los entornos operativos de la tecnología de la información. [AD 2-28]

Según el AD 2-28, la gestión del cambio también garantiza que se realicen cambios eficaces y eficientes mediante el uso de métodos y procedimientos que mejoren la calidad del entorno, lo que garantiza que los cambios sean transparentes para los clientes (es decir, los departamentos de la Ciudad) minimizando las interrupciones, y que exista un registro auditable de la actividad de cambio. [AD 2-28]

El alcance de esta Dirección Administrativa se aplica a todos los departamentos, a todo el personal de TI de la Ciudad de Dallas y a todos los consultores contratados por la Ciudad de Dallas que diseñen, desarrollen, configuren, instalen, operen, mantengan o soliciten cambios en la tecnología de la información. [AD 2-28]

El AD 2-28 define el alcance de los cambios controlados por la Gestión de Cambios para incluir cualquier modificación o mejora realizada en todos y cada uno de los entornos de Producción de TI. Los ejemplos incluyen, pero no se limitan a:

- Equipos informáticos (por ejemplo, ordenadores de sobremesa, portátiles, servidores, ordenadores centrales);
- Equipos informáticos móviles (por ejemplo, PDA, tabletas, MDC);
- Aplicaciones informáticas, sistemas operativos y servicios que prestan;

- Sistemas de gestión de bases de datos y definiciones de estructuras de datos;
- Servicios de computación distribuidos, basados en la web o en la nube;
- Equipos y servicios de redes de datos (por ejemplo, LAN, WAN, Wi-Fi, radio, Internet);
- Equipos y servicios de telecomunicaciones (por ejemplo, VoIP, IVR, 911, radio, Smartphone),
- Infraestructura física de apoyo a la TI (por ejemplo, cableado, servicio eléctrico, HVAC, control de acceso). [AD 2-28]

El AD 2-28 define varios términos y funciones dentro del proceso de gestión del cambio. Entre los más importantes de esta dirección están:

- Gestor del Cambio, que es un rol que identifica a los recursos responsables de la administración de los procesos y actividades de la Gestión del Cambio. El Gestor de Cambios administra el proceso global de gestión de cambios e interactúa con cada una de las demás partes implicadas.
- Iniciador de la solicitud, que presenta las solicitudes de cambio, aclara la información y realiza las pruebas de aceptación.
- La Junta Consultiva de Cambios está compuesta por personal de la empresa y de ITS. La Junta revisa y aprueba o rechaza las solicitudes de cambios en consonancia con la estrategia técnica o empresarial, el Costo y el riesgo. La Junta también prioriza el orden de despliegue de los cambios.
- El probador de cambios identifica los recursos responsables de probar los cambios.
- La Junta de Control de Versiones está compuesta por personal de gestión de ITS y se encarga de revisar todas las solicitudes de cambio de versiones para comprobar el riesgo técnico y la preparación. La Junta aprueba o rechaza todas las implantaciones en producción.
- Por último, el ejecutor del cambio revisa la documentación de apoyo y despliegue, y despliega los cambios en el entorno informático. [AD 2-28]

31.5 AD 2-34 - Política, Normas y Procedimientos de Copia de Seguridad y Recuperación de Datos

La Dirección Administrativa 2-34 (AD 2-34) Política, Norma y Procedimientos de Copia de Seguridad y Recuperación de Datos establece que todas las aplicaciones y sistemas de Tecnología de la Información deben planificar su recuperación mediante el establecimiento de procedimientos de copia de seguridad

y retención de aplicaciones y datos. Este documento está pensado como referencia para otros departamentos de la Ciudad. El AD 2-34 exige que todos los departamentos de la Ciudad de Dallas establezcan normas mínimas para la realización de copias de seguridad y la conservación de sus sistemas de tecnología de la información y bases de datos. [AD 2-34]

El propósito del AD-34 es definir la política, las normas mínimas y los procedimientos para la realización de copias de seguridad y recuperación de los sistemas de hardware y software de tecnología de la información y los datos utilizados en la Ciudad de Dallas para el Departamento de Servicios de Información y Tecnología. Además, el AD-34 define las normas y procedimientos mínimos recomendados para la realización de copias de seguridad y recuperación para otros departamentos de la Ciudad de Dallas. [AD-34]

El documento AD 2-34 define las funciones de los gestores de TI dentro del Departamento de Servicios de Información y Tecnología:

- Incorporar la copia de seguridad y la recuperación en todos los diseños de aplicaciones de hardware y software de acuerdo con los requisitos de copia de seguridad y retención del propietario de los datos;
- Garantizar que los procedimientos de copia de seguridad están creados, completos y documentados para que el Centro de Datos los siga;
- Documentar todos los procedimientos de copia de seguridad y recuperación según los requisitos del propietario de los datos;
- Probar los sistemas de copia de seguridad con el propietario de los datos antes de implementarlos en la producción; y
- Verificar, hacer correcciones y entregar los procedimientos y responsabilidades de las copias de seguridad al Centro de Datos. [AD 2-34]

El AD 2-34 establece que los departamentos clientes propietarios de los datos:

- Definir todas las políticas y procedimientos de copia de seguridad y conservación antes de su aplicación;
- Revisar todos los resultados de las pruebas de seguridad con el CIS antes de su aplicación,

- Notificar al Departamento de Servicios de Información y Tecnología cualquier cambio en los requisitos de conservación de copias de seguridad. [AD 2-34]

En la aplicación de los procedimientos del AD 2-34, los procedimientos establecen que los departamentos propietarios de los datos son responsables del desarrollo de sus políticas, procedimientos y normas de copia de seguridad y conservación. Sin embargo, el AD 2-34 establece que el Departamento de Servicios de Información y Tecnología puede ayudar a los departamentos en la aplicación de estas políticas, procedimientos y normas. [AD 2-34]

El AD 2-34 establece además que todos los procedimientos de copia de seguridad y recuperación de datos deberán ser documentados por el departamento propietario y probados por éste con la asistencia y revisión del Departamento de Servicios de Información y Tecnología antes de su aplicación. [AD 2-34]

La norma AD 2-34 define las condiciones físicas (es decir, temperatura y humedad) para el almacenamiento de las copias de seguridad. También exige la documentación de los programas de copias de seguridad y el etiquetado adecuado de determinadas copias de seguridad.

Por último, en caso de que un departamento necesite una restauración, el departamento hará una solicitud al Departamento de Servicios de Información y Tecnología, que documentará la información sobre el solicitante de la restauración y completará la restauración. [AD 2-34]

Sección VIII- Apéndices

Los siguientes apéndices proporcionan información y fuentes de información que se consideran beneficiosas para que el lector obtenga un contexto de las operaciones de TI proporcionadas por el ITS de la Ciudad.

32 Apéndice A - Gobernanza y Gestión de Datos

32.1 Asociación de Gestión de Datos (DAMA) Internacional

Resumen ejecutivo

"Los datos son el petróleo del siglo XXI". Estas sucintas palabras de Peter Sondergaard, director de Gartner Research, reflejan la creciente importancia que se concede a los datos. La industria ha comprendido que los datos serán el recurso que dirigirá la economía en los próximos años. [Datos e información son sinónimos y se han utilizado indistintamente en este documento].

La Ciudad de Dallas ha estado trabajando en los últimos años para utilizar los datos como un valioso recurso para mejorar los servicios prestados y disponibles para los Ciudadanos. Las iniciativas relativas a las Ciudades Inteligentes y el Portal de Datos Abiertos son sólo algunos ejemplos del uso de los datos. Siguiendo el objetivo de maximizar el valor y la disponibilidad de los datos, la Ciudad pondrá en marcha una estrategia de gestión de datos

32.1.1 Introducción

La gestión de datos es una disciplina relativamente nueva en comparación con las disciplinas tradicionales de gestión de activos, como la gestión financiera y la gestión de capital. La Ciudad debe liderar esta área crítica de rápido desarrollo. La Ciudad de Dallas ha elegido el marco de conocimientos de gestión de datos de la Asociación de Gestión de Datos (DAMA DMBOK, por sus siglas en inglés) para la gestión de este nuevo tipo de activos. Se eligió el marco de la DAMA porque se trata de un consenso impulsado por el mayor cuerpo de profesionales de datos del mundo que no está afiliado a ningún proveedor o tecnología específica. Los términos y definiciones de gestión de datos de este documento se ajustan al DMBOK de DAMA. Un vocabulario común en el ámbito de la gestión de datos es importante para esta nueva disciplina, y DAMA, a través de su enfoque sin ánimo de lucro e impulsado por el consenso, ha creado la versión más aceptable del glosario en la industria. Aprovechando las definiciones existentes de DAMA, no se ha adjuntado un glosario a este documento.

Además de establecer un lenguaje común para la gestión de datos, el DMBOK de DAMA proporciona un marco de gestión de datos que es holístico y abarca todos los sectores. Cada organización es única, y

todos los sectores pueden no tener la misma relevancia dentro de las organizaciones, si es que la tienen. La priorización y la profundidad del enfoque en los sectores es algo que deben decidir las organizaciones.

32.1.2 Caso de Negocio:

La propuesta de valor de las estrategias de gestión de datos tiene claros beneficios. La aplicación de prácticas y normas sólidas de gestión de datos conduce a datos claros, documentados y eficaces, y reduce las responsabilidades que conllevan los datos sensibles. Una mejor calidad de los datos supone un ahorro de costos en las operaciones de la administración municipal.

Además de ahorrar costos y reducir riesgos, la gestión de datos puede mejorar la prestación de servicios a los Ciudadanos de Dallas:

- Garantizar la vinculación de los recursos de datos con los mandatos legislativos y los objetivos de la Ciudad.
- Mejorar la interoperabilidad y la integración de los sistemas.
- Aumentar la flexibilidad y la agilidad de la organización para satisfacer los requisitos cambiantes.
- Identificar las oportunidades de innovación.

Problemas que se producen sin una estrategia de gestión de datos común y centralizada:

- Los problemas comunes se abordan de forma diferente, si es que se abordan.
- La falta de una estrategia común da lugar a una costosa reinvención de las mejores prácticas, políticas y soluciones.
- Los enfoques individuales y no planificados pueden conducir a resultados menos deseables.

32.1.3 Metodología de desarrollo

Las estrategias de gestión de datos se crearon basándose en los principios de gestión de datos de la Ciudad de Dallas, guiados por las direcciones administrativas de la Ciudad y otras directrices de la Ciudad.

Objetivos de la Ciudad de Dallas:

Objetivos y rendimiento de Dallas 365

- Desarrollo económico
- Medio ambiente y sostenibilidad
- Rendimiento y gestión financiera del gobierno
- Soluciones para la vivienda y el sinhogarismo
- Seguridad pública
- Calidad de vida, arte y cultura
- Transporte e infraestructuras
- Mano de obra, educación e igualdad

Principios de datos de ITS:

- Gestionar los datos de la empresa como un activo de la Ciudad
- Permitir la apertura y la transparencia
- Compartir los datos para aumentar su valor
- Hacer respetar la privacidad y la seguridad
- Integrar definiciones de datos y normas comunes
- Colaborar para eliminar duplicidades
- Mejorar el gobierno de la Ciudad a través de la calidad de los datos

32.1.4 Gobernanza de los datos:

Definición: La gobernanza de los datos es la ejecución de la autoridad y el control (planificación, seguimiento y aplicación) sobre la gestión de los activos de datos.

La gobernanza de los datos afecta a todas las áreas de la gestión de datos e influye directamente en las estrategias de gestión de datos incluidas en este documento y les da prioridad. Es importante distinguir la gobernanza de los datos de la gobernanza de la TI; es diferente en el sentido de que se encuentra entre la gobernanza de la empresa y la de la TI. Por ejemplo, el cumplimiento de la Ley de Portabilidad y

Responsabilidad de los Seguros Médicos (HIPAA) implica la participación tanto del negocio como de la TI. En las organizaciones, las necesidades de datos están enmarcadas por el negocio y deben ser auditadas por el negocio para su cumplimiento y calidad, mientras que las TI implementan y operan la infraestructura para los datos. El gobierno de los datos debe ser una asociación que incluya a los administradores de la empresa, que deciden el uso y el control de los datos, y a los administradores de la tecnología, que permiten y administran el flujo y el almacenamiento de los datos. Los administradores de la empresa son los fiduciarios de los datos, mientras que los administradores de la tecnología son los guardianes de los datos. Los administradores empresariales y tecnológicos no son nuevos puestos de trabajo, sino una formalización de las funciones existentes en los distintos organismos, donde la gobernanza de los datos permitiría la toma de decisiones compartida sobre los activos de datos. La gestión de los problemas de los datos, cuando hay que tomar decisiones difíciles, es una actividad clave de la gobernanza de los datos.

La gobernanza de los datos se ocupa a menudo del uso de los mismos y de sus implicaciones legales. La asesoría jurídica es aconsejable en el seno del máximo órgano de gobierno de los datos para interpretar las leyes e intentar cambios, si es necesario, por el bien de los Ciudadanos de Dallas. Garantizar el cumplimiento de las leyes relativas a los datos es una parte esencial de la gobernanza de datos, lo que hace que la auditoría sea un componente esencial del Consejo de Gobernanza de Datos.

- **Estrategia:** Obtener el máximo apoyo ejecutivo posible a nivel municipal para la gobernanza de datos.
- **Estrategia:** Educar sobre la necesidad de gobernar los datos.
- **Estrategia:** Formar un grupo de trabajo para crear los derechos de decisión y las estructuras de responsabilidad para un Consejo de Gobernanza de Datos.
- **Estrategia:** Desarrollar una carta de gobierno de datos de la Ciudad basada en la colaboración, el apoyo mutuo y la transparencia.
- **Estrategia:** Incluir la representación de los Departamentos pertinentes y de otras áreas según sea necesario
- **Estrategia:** Formar un órgano de gobernanza de datos que proporcione apoyo de personal a la función de gobernanza de datos, facilite las reuniones, prepare los órdenes del día de las

reuniones y publique las actas.

32.1.5 Modelado y Diseño de Datos:

Definición: *Diseñar, implementar y mantener las soluciones para satisfacer las necesidades de datos de una organización.*

La práctica de analizar, diseñar, implementar y mantener productos de datos para una organización es el desarrollo de datos. Los productos de datos finales son modelos de datos, estructuras físicas de datos y productos finales de información, como pantallas e informes, todo ello con el objetivo de apoyar una serie de actividades empresariales que van desde el desarrollo de la estrategia hasta las operaciones. Las actividades de desarrollo de datos pueden incluir arquitectos de datos, arquitectos de soluciones, analistas de negocio, analistas de datos, desarrolladores de software, administradores de bases de datos, administradores de negocio y expertos en la materia (PYMES), todos trabajando juntos para producir los productos de datos. Dependiendo del tamaño del proyecto y de la organización, una o varias de estas funciones pueden recaer en una sola persona. El desarrollo de datos afecta a varias fases del ciclo de vida del desarrollo de sistemas (SDLC) en las que se definen, diseñan e implementan los datos, ya sea en el método tradicional de cascada o en las fases acortadas de las metodologías ágiles.

- ***Estrategia:*** *Invertir en un acuerdo empresarial sobre las definiciones de negocio para los elementos de datos críticos en las primeras fases de la recopilación de requisitos, hacia un glosario de negocio.*
- ***Estrategia:*** *Desarrollar normas y convenciones de denominación de entidades, atributos, y tablas y columnas.*
- ***Estrategia:*** *Los datos deben reflejar las entidades y atributos reales de la empresa y no estar vinculados a una aplicación específica. Implemente los requisitos específicos de la aplicación mediante la virtualización de datos utilizando vistas, procedimientos almacenados y funciones.*
- ***Estrategia:*** *El procesamiento de la base de datos debe ser empujado hacia el servidor de la base de datos por diseño en lugar del servidor de la aplicación.*
- ***Estrategia:*** *Aplicar las reglas de datos más cerca de la base de datos cuando sea posible, en lugar de en el código de la aplicación.*
- ***Estrategia:*** *Desarrollar datos de prueba que cumplan los requisitos de privacidad y*

confidencialidad.

- ***Estrategia:*** *Considerar la implementación de prácticas de revisión de SQL entre las funciones del desarrollador y del DBA para prevenir fallos de producción, mejorar el rendimiento y mejorar la capacidad de mantenimiento.*
- ***Estrategia:*** *Automatizar al máximo la migración de datos de las plataformas de origen a las de destino en las primeras fases de desarrollo.*
- ***Estrategia:*** *Tener la política de no actualizar los datos de producción directamente a través de actualizaciones ad-hoc.*
- ***Estrategia:*** *Formar de forma cruzada, según proceda, a los DBA en tecnologías no relacionales como XML, XML Schema, Namespaces y a los desarrolladores OO en las mejores prácticas de SQL utilizando bases de datos relacionales.*

32.1.6 Almacenamiento de Datos y Operaciones:

Definición: *La planificación, el seguimiento, el control y el apoyo de los activos de datos estructurados a través del ciclo de vida de los activos de datos.*

La gestión de operaciones de bases de datos es una de las áreas más maduras de la gestión de datos, con las mejores prácticas probadas durante décadas y perfeccionadas por grandes redes de profesionales, principalmente administradores de bases de datos. La gestión de operaciones de bases de datos abarca dos áreas principales a) el soporte de las bases de datos y b) la gestión de la tecnología de datos. Los administradores de bases de datos, en coordinación con otras funciones de TI, intentan maximizar el valor de los activos de datos estructurados de la organización a) protegiendo y garantizando la integridad de los datos, b) maximizando la disponibilidad de los datos y c) optimizando el rendimiento de las bases de datos. Estos objetivos se apoyan a través de muchas actividades como:

- Planificación y gestión de copias de seguridad y recuperación
- Supervisión y ajuste de la base de datos
- Garantizar que se utilizan las versiones adecuadas de las tecnologías de bases de datos
- Ejecución de diversas operaciones de datos, como la carga, la reorganización de las bases de datos, la actualización de las estadísticas de datos, el archivo y la depuración
- Evaluar las nuevas tecnologías de datos apropiadas para la organización

La administración de bases de datos, además de ser fundamental para la función de operaciones de bases de datos, desempeña un papel importante en otras áreas de gestión de datos, como el desarrollo de datos y la gestión de la seguridad de los mismos.

- ***Estrategia:*** *La política y las normas de archivo de datos deben desarrollarse y seguirse para evitar que la sobrecarga de las bases de datos de producción provoque una degradación del rendimiento con el tiempo.*
- ***Estrategia:*** *Debe desarrollarse y seguirse la política de purga de datos en consonancia con el Calendario de Retención de la Ciudad de Dallas y las necesidades de la empresa. Esto no debe confundirse con la política de archivo, ya que el archivo y la purga son dos actividades distintas.*
- ***Estrategia:*** *Las organizaciones deben verificar la validez de sus copias de seguridad mediante ejercicios de recuperación al menos una vez al año.*
- ***Estrategia:*** *La política de cambios en la base de datos de producción debe exigir siempre un plan de retirada documentado para cada cambio.*
- ***Estrategia:*** *Tener una política para probar siempre los cambios en entornos de prueba, a excepción de las emergencias*
- ***Estrategia:*** *Tener una política para desarrollar las habilidades de automatización dentro de la comunidad de DBA.*
- ***Estrategia:*** *La desnormalización de la base de datos debería estar entre las estrategias de rendimiento menos preferidas dentro de las bases de datos de procesamiento de transacciones en línea (OLTP).*
- ***Estrategia:*** *Invertir en la práctica de actividades de prueba de concepto para tecnologías nuevas y prometedoras con el fin de crear una lista de tecnologías adecuadas por adelantado. Esto ayudaría a evitar la sobreestimación de los beneficios y la subestimación de los costos cuando surjan oportunidades de aplicación.*
- ***Estrategia:*** *Decidir y documentar la política de actualización del software de gestión de bases de datos, incluso si la política se limita a reaccionar ante los ultimátums de fin de soporte del proveedor. Una política de actualización documentada redunda en una mejor planificación de los recursos de infraestructura.*

32.1.7 Gestión de la seguridad de los datos:

Definición: Planificación, desarrollo y ejecución de políticas y procedimientos de seguridad de datos para proporcionar una autenticación, autorización, acceso y auditoría adecuados de datos e información.

No es el tamaño de la organización, sino la naturaleza del negocio lo que dicta el esfuerzo necesario para la gestión de la seguridad de los datos. Las organizaciones que manejan información personal sensible tendrían que invertir más que otras en la gestión de la seguridad de los datos. Hay que mantener un equilibrio adecuado entre el acceso a los datos y su seguridad. Unas políticas de seguridad férreas pueden ahogar los usos beneficiosos de los datos y generar resentimiento dentro de una organización. La seguridad de los datos, gestionada cuidadosamente con supervisión, auditoría y aplicación, promueve la confianza entre las partes interesadas. Esta confianza fomenta el intercambio de datos y, por tanto, aumenta su valor. Las organizaciones serán reacias a compartir información a menos que se garantice una gestión adecuada de la seguridad de los datos. La seguridad de los datos debe tener una gobernanza juiciosa con las partes interesadas, de modo que resulte práctico su seguimiento diario a nivel operativo.

La tendencia de la computación en la nube trae consigo preocupaciones especiales sobre la seguridad de los datos. Las organizaciones pueden trasladar a la nube los datos y los controles de seguridad asociados, pero no la responsabilidad. Debe prestarse especial atención a los datos que se trasladan a la nube y al contenido contractual con el proveedor de la misma.

- ***Estrategia:*** *Basándose en las clasificaciones de seguridad de los datos, las organizaciones deben abordar los datos sensibles expuestos en las bases de datos de prueba mediante el enmascaramiento o la desidentificación de los datos.*
- ***Estrategia:*** *Desarrollar plantillas de acuerdos de intercambio de datos que las organizaciones puedan aprovechar al elaborar el intercambio de datos entre organismos.*
- ***Estrategia:*** *Las organizaciones con datos sensibles deben gestionar, a cierto nivel, un registro de*

los accesos concedidos a las funciones y a los individuos.

- ***Estrategia:*** *Se debe evitar el acceso a datos sensibles a través de cuentas compartidas.*
- ***Estrategia:*** *Gestionar el acceso a través de la seguridad basada en roles a nivel de grupo en lugar de cuentas individuales. Asignar individuos a los roles.*
- ***Estrategia:*** *Conceder el acceso a los datos sensibles a través de la aprobación y no a través del opt-in por defecto.*
- ***Estrategia:*** *Para la información muy sensible, prever la autenticación y el control de acceso de los patrones inusuales con un equilibrio judicial de la automatización y los controles humanos.*
- ***Estrategia:*** *Incorporar procesos de auditoría anuales no enmarcados en una mentalidad de búsqueda de fallos, sino con un objetivo de seguimiento para la mejora continua.*
- ***Estrategia:*** *Desarrollar una estrategia de seguridad de datos en la nube.*

32.1.8 Gestión de Referencias y Datos Maestros:

Definición: Actividades de planificación, ejecución y control para garantizar la coherencia con una "versión dorada" de los valores de los datos contextuales.

Todo registro de transacción comercial necesita un contexto. Por ejemplo, cuando un cliente hace un pedido de una determinada cantidad de productos, a un determinado precio, el cliente, el producto y el estado del pedido son datos contextuales, mientras que la cantidad del pedido, el descuento y el precio son datos de la transacción. Las organizaciones se enfrentan al reto de mantener la coherencia de los datos contextuales en todas las líneas de negocio y sistemas. Los datos contextuales mantenidos en silos dificultan la integración de la organización con las inevitables incoherencias. El análisis de la causa raíz de muchos problemas de calidad de datos en las organizaciones apunta a la necesidad de integrar los datos maestros y de referencia. La calidad general de los datos en muchas organizaciones está directamente correlacionada con la calidad de los datos contextuales. La gestión de datos maestros y de referencia son esencialmente programas de calidad de datos en los niveles superiores de la organización.

Hay dos tipos de datos contextuales, los datos de referencia y los datos maestros. En el ejemplo anterior,

la información sobre el cliente y el producto son datos maestros, mientras que el estado del pedido es el dato de referencia. Los datos de referencia suelen aparecer como una lista de selección dentro de las aplicaciones. Los datos de referencia categorizan los datos con fines empresariales y, por lo tanto, los valores del dominio tienen que ser controlados con definiciones para cada valor y con su relación con otros valores con el dominio. Los datos maestros, una vez definidos a nivel de entidad, no requieren la definición de cada elemento. Sin embargo, el reto de los datos maestros es la prevención de duplicados y la creación de un registro "de oro" con la fusión o los elementos más precisos de fuentes dispares, y la posterior difusión de los datos maestros. Las estructuras de gobernanza son esenciales para los proyectos de gestión de datos maestros y de referencia, porque los conflictos de datos no siempre pueden resolverse mediante la automatización y los procedimientos establecidos.

- ***Estrategia:*** *Identificar posibles COIs dentro del gobierno de la Ciudad que puedan beneficiarse de los esfuerzos de gestión de datos maestros (MDM).*
- ***Estrategia:*** *Desarrollar metadatos robustos, incluyendo un glosario de negocio, al principio de un esfuerzo de MDM frente a la documentación al final.*
- ***Estrategia:*** *Planificar la gobernanza de los datos como algo imprescindible, no opcional, al abordar un proyecto de gestión de datos de referencia o maestros.*
- ***Estrategia:*** *Invertir en los esfuerzos de gestión de datos maestros y de referencia como un programa continuo y no como un proyecto con fecha de finalización.*
- ***Estrategia:*** *Invertir en esfuerzos de gestión de datos maestros y de referencia en iteraciones más pequeñas para ofrecer y demostrar el valor y el apoyo continuo de las partes interesadas.*

32.1.9 Gestión de Almacenes de Datos, Big Data e Inteligencia Empresarial:

Definición: *La gestión de almacenes de datos e inteligencia empresarial (DW-BIM) abarca las actividades de planificación, implementación y control en la recopilación, limpieza, integración y presentación de datos a los trabajadores del conocimiento para el análisis empresarial, permitiendo así la toma de decisiones informadas por parte de las organizaciones.*

El almacenamiento de datos es la actividad que se ocupa de la recopilación de datos de diversas fuentes

de datos dentro de la organización, integrándolos y almacenándolos como una instantánea de las operaciones de la organización en diferentes momentos. En otras palabras, se trata de contenidos de datos empresariales integrados con una perspectiva histórica. El BIM es la parte complementaria de la utilización de este contenido de datos mediante diversas herramientas. Estas dos actividades están entrelazadas en el sentido de que una es ineficaz sin la gestión de la calidad en la otra.

El uso principal del concepto de almacén de datos se está aplicando en la Ciudad mediante el uso de Big Data.

- ***Estrategia:*** *Aprovechar y apoyar las funciones del componente de gestión de datos, como la gestión de datos de referencia y maestros, la gobernanza de datos, la calidad de datos y la gestión de metadatos.*
- ***Estrategia:*** *cuando sea posible, buscar y colaborar con los profesores e investigadores de Big Data y Data Mining de las universidades cercanas*
- ***Estrategia:*** *Apoyar activamente e invertir en la política y los procesos de metadatos dentro de la organización con el proceso de glosario empresarial entre los pasos iniciales*
- ***Estrategia:*** *Resumir y optimizar al final, no al principio. Empezar a construir con los datos detallados.*

32.1.10 Gestión de Documentos y Contenidos:

Definición: La gestión de documentos y contenidos son las actividades de planificación, implementación y control para almacenar, proteger y acceder a datos no estructurados dentro de archivos electrónicos y registros físicos que incluyen texto, gráficos, imágenes, audio y vídeo.

Esta área se refiere a los datos no estructurados que no tienen el formato estructurado de los sistemas tradicionales de gestión de datos (relacionales, jerárquicos, de objetos, en red, etc.). Aunque las actividades de "almacenamiento, protección y acceso" dentro de la gestión de documentos y contenidos pueden parecer implicar un enfoque operativo, es muy importante considerar los aspectos estratégicos del gobierno de los datos, la arquitectura, la seguridad, la privacidad y la confidencialidad, los metadatos

y la clasificación, y la calidad de los datos. La gestión de documentos está más relacionada con el almacenamiento, el inventario y el control de los documentos en papel o electrónicos mediante procesos y tecnologías, mientras que la gestión de contenidos se refiere a los procesos y tecnologías que se ocupan de la organización, la categorización y el acceso al contenido de esos documentos y registros. Hoy en día, la gestión de contenidos es especialmente importante para la gestión de contenidos en sitios y portales web. La gestión de documentos y la de contenidos, aunque distintas, se confunden a veces en la práctica, ya que los procesos empresariales y las funciones se entremezclan y los proveedores ofrecen productos que cubren ambas áreas. Esto se refleja en la estrategia de gestión de contenidos empresariales del Departamento de Sistemas de Información y en los documentos de estrategia de vídeo, que proporcionan más detalles sobre las estrategias mencionadas en este documento (disponibles en el grupo de Arquitectura Empresarial del DIS si se solicita).

- ***Estrategia:*** Identificar y documentar los principales tipos de datos no estructurados almacenados en la Ciudad.
- ***Estrategia:*** Documentar los requisitos de copia de seguridad y recuperación de los datos no estructurados
- ***Estrategia:*** *Sobre la base de los requisitos del documento AD 2-25, garantizar que los propietarios de los datos hayan clasificado correctamente los datos del departamento y hayan proporcionado cualquier control o requisito a los custodios de datos de ITS.*
- ***Estrategia:*** *Validar los requisitos de almacenamiento, las métricas de rendimiento del almacenamiento y otras actividades de mejores prácticas para almacenar y mantener los datos no estructurados*
- ***Estrategia:*** Garantizar auditorías periódicas de los controles de los datos de contenido para asegurar que se siguen las Políticas y Normas de datos requeridas basadas en los procedimientos necesarios para garantizar que los datos se almacenan, protegen y mantienen para la Ciudad.
- ***Estrategia:*** Garantizar la existencia de controles de seguridad adecuados para asegurar la privacidad de los datos y el control del acceso en función de los requisitos normativos, departamentales o de otro tipo basados en la clasificación de los datos.

32.1.11 Gestión de Metadatos:

Definición: La gestión de metadatos es el conjunto de procesos que garantizan la creación, el almacenamiento, la integración y el control adecuados para apoyar el uso asociado de los metadatos.

La falta de metadatos es una molestia para las organizaciones grandes y pequeñas. La falta de metadatos significativos y mantenidos conduce a ineficiencias tales como 1) mayores costos de reciclaje con la rotación de mano de obra/proveedores 2) mayor tiempo de comercialización de soluciones y cambios de sistema 3) más tiempo dedicado a la investigación por parte de los analistas de datos que validan o informan de los datos 4) decisiones empresariales incorrectas basadas en la falta de comprensión de los datos, 5) falta de entendimiento entre la empresa y las TI. Por ejemplo, los metadatos suelen formar parte de la lista de deseos aplazados de los gestores de aplicaciones que mantienen las soluciones, pero se convierten en algo imprescindible durante los cambios importantes.

Los metadatos son algo más que el diccionario de datos extraído de las bases de datos físicas o los modelos de una herramienta de modelado de datos. Es una amalgama de conocimientos técnicos y empresariales sobre los datos necesarios para el funcionamiento de la organización. No hay límites que dicten la "cantidad correcta" de metadatos y todo depende de cada caso. La cantidad de información técnica y empresarial sobre los elementos de datos debe ser proporcional a su importancia dentro de una organización. Los metadatos pueden estar compuestos por metadatos empresariales, operativos, técnicos, de proceso o de administración.

Es posible que las organizaciones independientes no dispongan de los recursos necesarios para invertir en la investigación y aplicación de las mejores prácticas, políticas y procedimientos en este ámbito. Este es un ámbito en el que el trabajo en colaboración puede ser de gran ayuda, en toda la Ciudad. No obstante, cabe señalar que, aunque las organizaciones han reconocido la importancia de mantener los metadatos, el índice de éxito, históricamente, es bajo, lo que indica que puede ser un programa difícil de aplicar.

- ***Estrategia:*** *Un grupo de metadatos para desarrollar la estrategia de metadatos debería estar*

entre las primeras áreas que se aborden a través de la gobernanza de datos.

- ***Estrategia:*** *Centrarse en la gobernanza de los metadatos para conseguir metadatos de alta calidad, el aspecto más importante para el éxito de cualquier programa de metadatos.*
- ***Estrategia:*** *Empezar en pequeño (pero escalable) a nivel local con los elementos más críticos del negocio.*
- ***Estrategia:*** *Para cada esfuerzo, articular el problema y/o el riesgo que impulsa el esfuerzo de gestión de metadatos.*
- ***Estrategia:*** *Explorar herramientas adecuadas para la gestión de metadatos, ya sean internas o comerciales, para facilitar la integración, la accesibilidad y el mantenimiento de los metadatos.*

32.1.12 Gestión de la Calidad de los Datos:

Definición: La gestión de la calidad de los datos son las actividades de planificación, ejecución y control que aplican técnicas de gestión de la calidad de los datos para medir, evaluar, mejorar y garantizar la idoneidad de los datos para su uso.

En el concepto de gestión de la calidad de los datos es fundamental la especificación de las necesidades de datos, la determinación de los métodos óptimos para medirlos y supervisarlos, el acuerdo de los niveles aceptables y las correcciones de la causa raíz cuando se produce una desviación de los niveles aceptables. El umbral de calidad aceptable para la empresa debe determinarse cuidadosamente y no fijarse en un nivel tan estricto que resulte demasiado costoso y, por tanto, inviable para la organización. La gestión de la calidad de los datos no es un esfuerzo único, sino un programa continuo de supervisión y corrección. Con un objetivo de mejora continua, el umbral aceptable de calidad de datos debe ser siempre un objetivo móvil. La aparición de iniciativas de gestión de datos maestros y de referencia dentro de las organizaciones ha fomentado la necesidad de gestionar la calidad de los datos y el uso de herramientas de calidad de datos COTS. La Ciudad debe promover la concienciación sobre la gestión de la calidad de los datos y las herramientas que ayudan en el proceso.

- ***Estrategia:*** *Desarrollar y mantener un inventario de herramientas de calidad de datos en la Ciudad con licencias de uso y costo.*

- ***Estrategia:*** *Promover la concienciación mediante la educación sobre las funciones de la herramienta de calidad de datos, las historias de éxito del gobierno de la Ciudad, la necesidad de estandarización de direcciones y la calidad.*
- ***Estrategia:*** *Intentar detener la proliferación de ofertas de múltiples proveedores en aras de*
- *de reducir los costos globales.*
- ***Estrategia:*** *Siempre que sea posible, seguir las normas de datos de la industria y federales.*

32.1.13 Implementación Táctica de la Gestión y Gobernanza de Datos

- Construir una visión y un alcance claros para la iniciativa de gobernanza de datos, de modo que se pueda garantizar que la organización pueda cumplir sus expectativas.
- Definir las normas y asignar la razón de ser de cada una de ellas. Describir los beneficios que se pueden obtener y el nivel de calidad que debe alcanzarse para obtenerlos. Crear métricas que muestren si los beneficios se están realizando.
- Diseñar un programa de gobierno de datos que sea adecuado para gestionar las normas definidas. Esto incluye la asignación de funciones y responsabilidades para los procesos utilizados para gestionar las actividades, como la gestión de cambios para las normas, y los cambios en cualquier proceso externo que afecte a la capacidad de gobierno de la organización, incluido el proceso de gestión de proyectos de TI.
- Contratar a un propietario de los datos para que se haga cargo de las normas y construya/supervise la hoja de ruta de la calidad de los datos.
- Construir la hoja de ruta de la calidad de los datos y documentar los niveles de calidad actuales. Medirla con respecto a los requisitos y proponer acciones para reducir la brecha y/o mantener una buena calidad.
- Llenar los roles de gobierno de datos restantes para operar el cumplimiento continuo. Medir y gestionar las actividades identificadas en la hoja de ruta de la calidad de los datos.

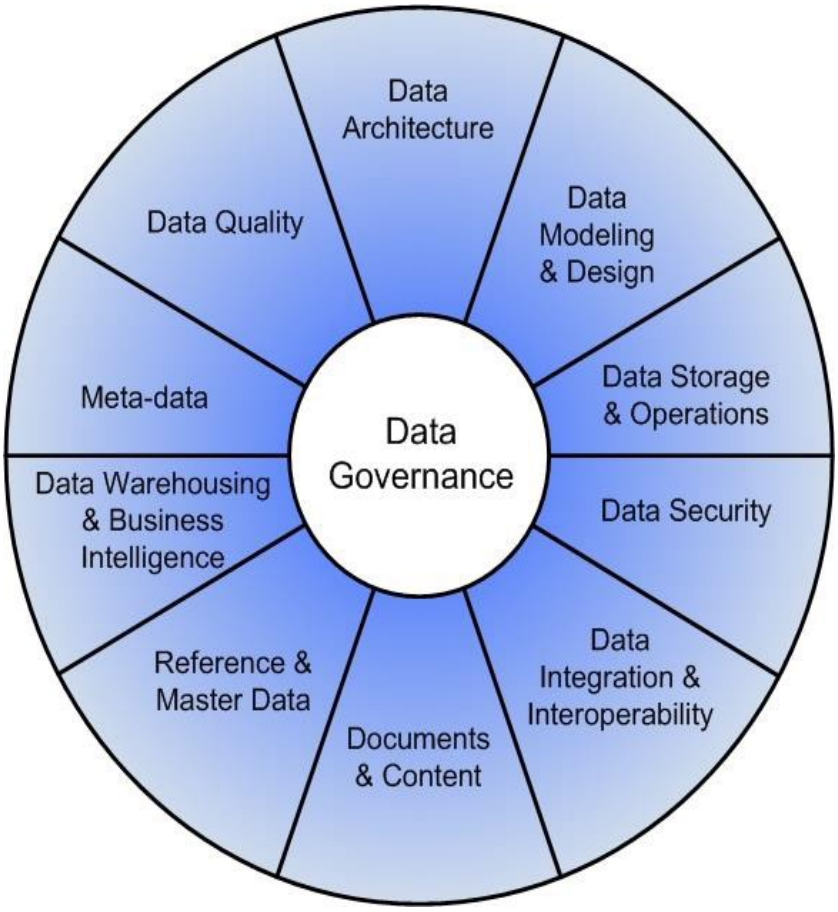
32.2 Marco de Conocimientos de Gestión de datos (DMBOK)

[Fuente primaria DAMA-DMBOK2 Framework 2014 DAMA International]

La gestión de datos es un término global que describe los procesos utilizados para planificar, especificar, habilitar, crear, adquirir, mantener, utilizar, archivar, recuperar, controlar y depurar datos. Estos procesos se solapan e interactúan dentro de cada área de conocimiento de la gestión de datos.

32.2.1 Marco Propuesto

DAMA define 11 áreas de conocimiento en el marco DAMA-DMBOK2 para la gestión de datos. Éstas se representan en la figura siguiente:



Las 11 áreas de conocimiento de la gestión de datos son:

- Gobernanza de los datos: planificación, supervisión y control de la gestión de los datos y del uso de los datos y de los recursos relacionados con ellos.
- Arquitectura de datos: la estructura general de los datos y los recursos relacionados con los datos como parte integrante de la arquitectura empresarial.
- Modelado y diseño de datos: análisis, diseño, construcción, pruebas y mantenimiento.
- Almacenamiento y operaciones de datos: despliegue y gestión del almacenamiento de activos de datos físicos estructurados.
- Seguridad de los datos: garantizar la privacidad, la confidencialidad y el acceso adecuado.
- Integración e interoperabilidad de datos: una nueva área de conocimiento para el DMBOK2. Adquisición, extracción, transformación, movimiento, entrega, replicación, federación, virtualización y soporte operativo de la integración de datos entre sistemas y actividades funcionales.
- Documentos y contenidos: almacenar, proteger, indexar y permitir el acceso a los datos que se encuentran en fuentes no estructuradas, y hacer que estos datos estén disponibles para su integración e interoperabilidad con los datos estructurados (bases de datos).
- Datos maestros y de referencia: gestión de los datos compartidos para reducir la redundancia y garantizar una mejor calidad de los datos a través de la definición estandarizada y el uso de valores de datos.
- Almacenamiento de datos e inteligencia empresarial: gestionar el procesamiento de datos analíticos y permitir el acceso a los datos de apoyo a la toma de decisiones para la elaboración de informes y análisis
- Metadatos: recopilación, categorización, mantenimiento, integración, control, gestión y entrega de metadatos.
- Calidad de los datos: definir, supervisar, mantener la integridad de los datos y mejorar su calidad.

32.2.2 Resumen

En resumen, el objetivo de esta sección ha sido introducir y proporcionar una visión general de alto nivel del Marco de Gestión de Datos DMBOK2 y las áreas de conocimiento asociadas. El marco es una guía

flexible que permite a las entidades trabajar dentro de sus requisitos internos de gestión de datos para proporcionar un conjunto de áreas comunes aprobadas por la industria para crear políticas, normas y procedimientos para la Gobernanza de Datos y su implementación.

33 Apéndice B - Gestión de servicios de TI

La gestión de servicios de TI es un enfoque de la gestión de la tecnología de la información que se centra en la entrega de valor empresarial a través de los servicios.

La Ciudad de Dallas ha adoptado ITILv3 como su marco de gestión de servicios de TI (ITSM). ITILv3 se compone de 26 procesos que apoyan la prestación de servicios de TI para lograr los resultados empresariales deseados. En la actualidad, ITS sólo opera parcialmente tres de los 26 procesos disponibles.

33.1 Servicios

Los servicios son un medio de aportar valor a los clientes facilitando los resultados que éstos desean conseguir sin tener que asumir costos y riesgos específicos. Los servicios facilitan los resultados mejorando la realización de las tareas asociadas y reduciendo el efecto de las limitaciones. Estas limitaciones pueden incluir la regulación, la falta de financiación o capacidad, o la limitación de la tecnología. El resultado es un aumento de la probabilidad de obtener los resultados deseados. Mientras que algunos servicios mejoran el rendimiento de las tareas, otros tienen un impacto más directo: realizan la tarea en sí. [ITILv3]

ITILv3 ha definido un resultado como el resultado de llevar a cabo una actividad, seguir un proceso o prestar un servicio de TI. El término se utiliza para referirse a los resultados previstos, así como a los resultados reales.

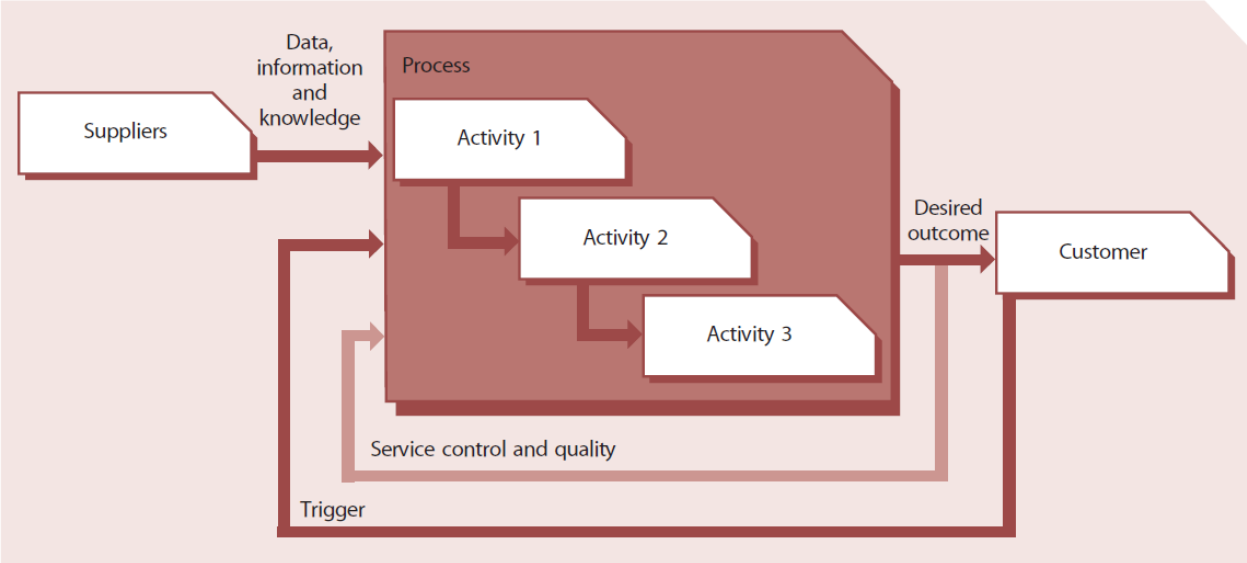


Figura 3Diagrama de procesos básicos de ITILv3

33.2 Gestión de Servicios

La gestión de servicios es un conjunto de capacidades organizativas especializadas para proporcionar valor a los clientes en forma de servicios. Las capacidades adoptan la forma de funciones y procesos para la gestión de los servicios a lo largo de su ciclo de vida, con especializaciones en estrategia, diseño, transición, funcionamiento y mejora continua. Las capacidades representan la capacidad, competencia y confianza de una organización de servicios para actuar. El acto de transformar los recursos en servicios valiosos es el núcleo de la Gestión de Servicios. Sin estas capacidades, una organización de servicios no es más que un conjunto de recursos que por sí mismo tiene un valor intrínseco relativamente bajo para los clientes. [ITILv3]

Las capacidades de las organizaciones están condicionadas por los retos que deben superar. Un ejemplo de ello es cómo en la década de 1950 Toyota desarrolló capacidades únicas para superar el reto de su menor escala y capital financiero en comparación con sus rivales estadounidenses. Toyota desarrolló nuevas capacidades en ingeniería de producción, gestión de operaciones y gestión de proveedores para compensar su incapacidad de permitirse grandes inventarios, fabricar componentes, producir materias primas o poseer las empresas que las producían. Las capacidades de gestión de servicios se ven influidas de forma similar por los siguientes retos que distinguen a los servicios de otros sistemas de creación de valor, como la fabricación, la minería y la agricultura: [ITILv3]

- La naturaleza intangible del resultado y los productos intermedios de los procesos de servicio; es difícil de medir, controlar y validar (o probar). [ITILv3]
- La demanda está estrechamente unida a los activos del cliente; los usuarios y otros activos del cliente como procesos, aplicaciones, documentos y transacciones llegan con la demanda y estimulan la producción de servicios. [ITILv3]
- Alto nivel de contacto para productores y consumidores de servicios; hay poca o ninguna barrera entre el cliente, el front-office y el back-office. [ITILv3]
- La naturaleza perecedera de la producción de servicios y de la capacidad de los mismos; para el cliente tiene valor la garantía de un suministro continuo de calidad constante. Los proveedores necesitan asegurar un suministro constante de la demanda de los clientes. [ITILv3]

Sin embargo, la gestión de servicios es algo más que un conjunto de capacidades. También es una práctica profesional respaldada por un amplio cuerpo de conocimientos, experiencia y habilidades. Una comunidad global de individuos y organizaciones de los sectores público y privado fomenta su crecimiento y madurez. Existen planes formales para la educación, la formación y la certificación de las organizaciones e individuos que la practican y que influyen en su calidad. Las mejores prácticas de la industria, la investigación académica y las normas formales contribuyen a su capital intelectual y se nutren de él. [ITILv3]

Los orígenes de la gestión de servicios se encuentran en las empresas de servicios tradicionales, como aerolíneas, bancos, hoteles y compañías telefónicas. Su práctica ha crecido con la adopción por parte de las organizaciones de TI de un enfoque orientado a los servicios para gestionar las aplicaciones, la infraestructura y los procesos de TI. Las soluciones a los problemas empresariales y el apoyo a los modelos, estrategias y operaciones de la empresa se presentan cada vez más en forma de servicios. La popularidad de los servicios compartidos y la subcontratación ha contribuido al aumento del número de organizaciones que son proveedores de servicios, incluidas las unidades organizativas internas. Esto, a su vez, ha reforzado la práctica de la Gestión de Servicios y, al mismo tiempo, le ha impuesto mayores retos. [ITILv3]

33.3 Funciones y Procesos a lo Largo del Ciclo de Vida

33.3.1 Funciones

Las funciones son unidades de las organizaciones especializadas en realizar determinados tipos de trabajo y responsables de resultados específicos. Son autónomas y cuentan con las capacidades y los recursos necesarios para su desempeño y sus resultados. Las capacidades incluyen métodos de trabajo internos a las funciones. Las funciones tienen su propio cuerpo de conocimientos, que se acumulan a partir de la experiencia. Proporcionan estructura y estabilidad a las organizaciones. [ITILv3]

Las funciones son un medio de estructurar las organizaciones para aplicar el principio de especialización. Las funciones suelen definir los roles y la autoridad y responsabilidad asociadas para un desempeño y unos resultados específicos. La coordinación entre funciones a través de procesos compartidos es un patrón común en el diseño de organizaciones. Las funciones tienden a optimizar sus métodos de trabajo a nivel local para centrarse en los resultados asignados. Una mala coordinación entre las funciones, combinada con un enfoque interno, conduce a silos funcionales que dificultan la alineación y la retroalimentación, fundamentales para el éxito de la organización en su conjunto. Los modelos de procesos ayudan a evitar este problema con las jerarquías funcionales, ya que mejoran la coordinación y el control entre funciones. Los procesos bien definidos pueden mejorar la productividad dentro y entre las funciones. [ITILv3]

33.3.2 Procesos

Los procesos son ejemplos de sistemas de bucle cerrado porque proporcionan el cambio y la transformación hacia un objetivo y utilizan la retroalimentación para la acción auto-reforzante y auto-correctiva (Diagrama de Proceso Básico de ITILv3 arriba). Es importante considerar el proceso completo o cómo un proceso encaja en otro. [ITILv3]

Las definiciones de los procesos describen las acciones, las dependencias y la secuencia. Los procesos tienen las siguientes características: [ITILv3]

- Son medibles. Las organizaciones son capaces de medir el proceso de manera relevante. Están orientados al rendimiento. Los gestores quieren medir el costo, la calidad y otras variables, mientras que los profesionales se preocupan por la duración y la productividad. [ITILv3]

- Tienen resultados específicos. La razón de ser de un proceso es ofrecer un resultado concreto. Este resultado debe ser individualmente identificable y contabilizable. Si bien podemos contar los cambios, es imposible contar cuántas mesas de servicio se completaron. [ITILv3]
- Entregan a los clientes. Todo proceso entrega sus resultados principales a un cliente o parte interesada. Pueden ser internos o externos a la organización, pero el proceso debe satisfacer sus expectativas. [ITILv3]
- Responden a un evento específico. Aunque un proceso puede ser continuo o iterativo, debe ser trazable a un desencadenante específico. [ITILv3]

A menudo se confunden las funciones con los procesos. Por ejemplo, hay ideas erróneas acerca de que la gestión de la capacidad es un proceso de Gestión de Servicios. En primer lugar, la gestión de la capacidad es una capacidad organizativa con procesos y métodos de trabajo especializados. Que sea o no una función o un proceso depende totalmente del diseño de la organización. Es un error asumir que la gestión de la capacidad sólo puede ser un proceso. Es posible medir y controlar la capacidad y determinar si es adecuada para un fin determinado. Asumir que es siempre un proceso con resultados discretos contables puede ser un error. [ITILv3]

33.4 Especialización y Coordinación a lo Largo del Ciclo de Vida

La especialización y la coordinación son necesarias en el enfoque del ciclo de vida. La retroalimentación y el control entre las funciones y los procesos dentro y entre los elementos del ciclo de vida lo hacen posible. El patrón dominante en el ciclo de vida es el progreso secuencial que comienza con la Estrategia del Servicio (SS), pasando por la Prestación del Servicio (SD), la Transición del Servicio (ST), la Operación del Servicio (SO) y volviendo al SS a través de la Mejora Continua del Servicio (CSI). Sin embargo, este no es el único patrón de acción. Cada elemento del ciclo de vida proporciona puntos de retroalimentación y control. [ITILv3]

La combinación de múltiples perspectivas permite una mayor flexibilidad y control en distintos entornos y situaciones. El enfoque del ciclo de vida imita la realidad de la mayoría de las organizaciones en las que una gestión eficaz requiere el uso de múltiples perspectivas de control. Los responsables del diseño, desarrollo y mejora de los procesos para la Gestión de Servicios pueden adoptar una perspectiva de control basada en los procesos. Para los responsables de la gestión de acuerdos, contratos y servicios puede ser mejor una perspectiva de control basada en el ciclo de vida con fases diferenciadas. Ambas

perspectivas de control se benefician del pensamiento sistémico. Cada perspectiva de control puede revelar patrones que pueden no ser evidentes en la otra. [ITILv3]

33.5 Una Perspectiva Histórica de la Gestión de Servicios de TI y los Orígenes de ITIL

La gestión de servicios de TI (ITSM) ha evolucionado de forma natural a medida que los servicios se han ido apuntalando con el tiempo gracias al desarrollo de la tecnología. En sus primeros años, las TI se centraban en el desarrollo de aplicaciones, ya que todas las nuevas posibilidades parecían ser un fin en sí mismas. Aprovechar las aparentes ventajas de estas nuevas tecnologías significaba concentrarse en la entrega de las aplicaciones creadas como parte de una oferta de servicios más amplia, que diera soporte al propio negocio. [ITILv3]

Durante la década de 1980, a medida que la práctica de la gestión de servicios crecía, también lo hacía la dependencia de la empresa. Satisfacer las necesidades del negocio exigía un reenfoque más radical para un enfoque de servicios de TI y surgió el "servicio de ayuda de TI" para hacer frente a la frecuencia de los problemas que sufrían quienes intentaban utilizar los servicios de TI en la prestación de su negocio. [ITILv3]

Al mismo tiempo, el gobierno del Reino Unido, impulsado por la necesidad de encontrar eficiencias, se propuso documentar cómo las mejores y más exitosas organizaciones abordaban la gestión de servicios. A finales de la década de 1980 y principios de la de 1990, se elaboró una serie de libros que documentaban un enfoque de la gestión de servicios de TI necesario para apoyar a los usuarios de la empresa. Esta biblioteca de prácticas se denominó Biblioteca de Infraestructura de TI - ITIL para sus amigos. [ITILv3]

La biblioteca original llegó a tener más de 40 libros e inició una reacción en cadena de interés en la comunidad de servicios de TI del Reino Unido. El término "gestión de servicios de TI" no se había acuñado en ese momento, pero se convirtió en un término común a mediados de la década de 1990, a medida que crecía la popularidad de ITIL. En 1991, se creó un foro de usuarios, el Foro de Gestión de la Información de TI (ITIMF), para reunir a los usuarios de ITIL con el fin de intercambiar ideas y aprender los unos de los otros, y con el tiempo cambiaría su nombre por el de Foro de Gestión de Servicios de TI (itSMF). En la actualidad, el itSMF cuenta con miembros en todo el mundo, ya que la popularidad de ITIL sigue creciendo. [ITILv3]

Se estableció una norma formal para ITSM, la norma británica 15000, basada en gran medida en las prácticas de ITIL, que fue seguida por varias normas nacionales en numerosos países. Desde entonces, se introdujo la Norma ISO 20000:2005, que obtuvo un rápido reconocimiento a nivel mundial. [ITILv3]

La siguiente revisión de ITIL comenzó a mediados de los años 90, hasta 2004. La versión 2 de ITIL, como se la conoce comúnmente, era un producto más específico -con nueve libros- que salvaba explícitamente la brecha entre la tecnología y el negocio, y con una orientación muy centrada en los procesos necesarios para prestar servicios eficaces al cliente empresarial. [ITILv3]

33.6 ITIL Hoy en Día

En 2004, el OGC puso en marcha la segunda gran iniciativa de actualización de ITIL, en reconocimiento de los enormes avances tecnológicos y de los nuevos retos a los que se enfrentan los proveedores de servicios de TI. Las nuevas arquitecturas tecnológicas, la virtualización y la subcontratación se convirtieron en un pilar de las TI y el enfoque basado en procesos de ITIL necesitaba ser renovado para abordar los desafíos de la gestión de servicios. [ITILv3]

Después de veinte años, ITIL sigue siendo el marco de trabajo más reconocido del mundo para la gestión de servicios de TI. Aunque ha evolucionado y cambiado su amplitud y profundidad, conserva los conceptos fundamentales de la práctica líder. [ITILv3]

33.7 ¿Por Qué Tiene Tanto Éxito ITIL?

ITIL se compone intencionadamente de un enfoque de sentido común para la gestión de servicios: hacer lo que funciona. Y lo que funciona es la adaptación de un marco común de prácticas que unen todas las áreas de la prestación de servicios de TI hacia un único objetivo: aportar valor al negocio. La siguiente lista define las características clave de ITIL que contribuyen a su éxito global: [ITILv3]

- No es propietaria: las prácticas de gestión de servicios de ITIL son aplicables en cualquier organización de TI porque no se basan en ninguna plataforma tecnológica en particular, ni en ningún tipo de industria. ITIL es propiedad del gobierno del Reino Unido y no está vinculada a ninguna práctica o solución comercial propietaria. [ITILv3]
- No es prescriptiva: ITIL ofrece prácticas sólidas, maduras y probadas con el tiempo que son aplicables a todo tipo de organizaciones de servicios. Sigue siendo útil y relevante en los

sectores público y privado, en los proveedores de servicios internos y externos, en las pequeñas, medianas y grandes empresas, y en cualquier entorno técnico. [ITILv3]

- Mejores prácticas: Las prácticas de gestión de servicios de ITIL representan las experiencias de aprendizaje y el liderazgo de pensamiento de los mejores proveedores de servicios del mundo. [ITILv3]
- Buenas prácticas: No todas las prácticas de ITIL pueden considerarse "mejores prácticas", y con razón. Para muchos, una mezcla de prácticas comunes, buenas y mejores es lo que da sentido y viabilidad al ITSM. En algunos aspectos, las mejores prácticas son el sabor del día. Todas las mejores prácticas se convierten en prácticas comunes con el tiempo, siendo reemplazadas por nuevas mejores prácticas. [ITILv3]

33.8 La Propuesta de Valor de ITIL

Todos los proveedores de servicios de alto rendimiento comparten características similares. Esto no es una coincidencia. Hay capacidades específicas inherentes a su éxito que demuestran de forma constante. Una capacidad fundamental es su estrategia. Si preguntáramos a un proveedor de servicios de alto rendimiento qué es lo que le hace distinguirse de sus competidores, nos diría que es su comprensión intrínseca de cómo aportan valor a sus clientes. Entienden los objetivos empresariales del cliente y el papel que desempeñan para que se cumplan esos objetivos. Una mirada más atenta revelaría que su capacidad para hacer esto no proviene de reaccionar a las necesidades del cliente, sino de predecirlas mediante la preparación, el análisis y el examen de los patrones de uso del cliente. [ITILv3]

La siguiente característica importante es el uso sistemático de prácticas de gestión de servicios que son receptivas, coherentes y medibles, y definen la calidad del proveedor a los ojos de sus clientes. Estas prácticas proporcionan estabilidad y predictibilidad e impregnan la cultura del proveedor de servicios. [ITILv3]

La última característica es la capacidad del proveedor de analizar y ajustar continuamente la prestación de servicios para mantener unos servicios estables, fiables pero adaptables y con capacidad de respuesta que permitan al cliente centrarse en su negocio sin preocuparse por la fiabilidad de los servicios de TI. [ITILv3]

En estas situaciones, se observa una asociación de confianza entre el cliente y el proveedor de servicios. Comparten riesgos y recompensas y evolucionan juntos. Cada uno sabe que desempeña un papel en el éxito del otro. [ITILv3]

Como proveedor de servicios, esto es lo que quiere conseguir. Como cliente, esto es lo que quiere en un proveedor de servicios. [ITILv3]

Mire por un momento a los proveedores de servicios de alto rendimiento del sector. Verá que la mayoría utiliza prácticas de gestión de servicios ITIL. Esto no es en absoluto una coincidencia. [ITILv3]

33.9 Las Prácticas de Gestión de Servicios de ITIL

Cuando abrimos un grifo, esperamos que salga agua. Cuando pulsamos un interruptor de la luz, esperamos que la luz llene la habitación. No hace muchos años estas cosas tan básicas no eran tan fiables como lo son hoy. Sabemos instintivamente que los avances tecnológicos los han hecho lo suficientemente fiables como para considerarlos una utilidad. Pero no es sólo la tecnología lo que hace que los servicios sean fiables. Es cómo se gestionan. Esto es la gestión de los servicios. [ITILv3]

El uso de las TI hoy en día se ha convertido en la utilidad de los negocios. Disponer simplemente de la mejor tecnología no garantizará una fiabilidad similar a la de los servicios públicos. Una gestión de servicios profesional, receptiva y orientada al valor es lo que aporta esta calidad de servicio a la empresa. [ITILv3]

El objetivo del marco de prácticas de Gestión del Servicio de ITIL es proporcionar servicios a los clientes empresariales que sean adecuados para el propósito, estables y que sean tan fiables, que la empresa los vea como una utilidad de confianza. [ITILv3]

ITIL ofrece una guía de mejores prácticas aplicable a todo tipo de organizaciones que prestan servicios a una empresa. Cada publicación aborda las capacidades que tienen un impacto directo en el rendimiento de un proveedor de servicios. La estructura de la práctica principal toma forma en un Ciclo de Vida del Servicio. Es iterativo y multidimensional. Garantiza que las organizaciones estén preparadas para aprovechar las capacidades en un área para aprender y mejorar en otras. Se espera que el núcleo proporcione estructura, estabilidad y fuerza a las capacidades de gestión de servicios con principios, métodos y herramientas duraderos. Esto sirve para proteger las inversiones y proporcionar la base necesaria para la medición, el aprendizaje y la mejora. [ITILv3]

Las orientaciones de ITIL pueden adaptarse para su uso en diversos entornos empresariales y estrategias organizativas. La orientación complementaria proporciona flexibilidad para implementar el núcleo en una amplia gama de entornos. Los profesionales pueden seleccionar la orientación complementaria según sea necesario para proporcionar tracción para el núcleo en un contexto empresarial determinado, al igual que los neumáticos se seleccionan en función del tipo de automóvil, el propósito y las condiciones de la carretera. Esto es para aumentar la durabilidad y portabilidad de los activos de conocimiento y para proteger las inversiones en capacidades de gestión de servicios. [ITILv3]

33.10 Navegar por el Ciclo de Vida de la Gestión de Servicios de ITIL

Antes de hablar de los principios de las prácticas de gestión de servicios de ITIL, es útil entender la estructura general del contenido y cómo están organizadas las áreas temáticas dentro de cada uno de los libros que componen las prácticas. [ITILv3]

Las prácticas de gestión de servicios de ITIL se componen de tres conjuntos principales de productos y servicios: [ITILv3]

- Prácticas de gestión de servicios de ITIL - orientación básica. [ITILv3]
- Prácticas de gestión de servicios de ITIL - orientación complementaria. [ITILv3]
- Servicios de soporte web de ITIL. [ITILv3]

El debate de la Ciudad sobre la gestión de servicios de ITIL se centrará únicamente en las áreas de práctica de orientación básica.

Prácticas de Gestión del Servicio ITIL - Orientación básica

El conjunto básico consta de seis publicaciones: [ITILv3]

- Introducción a las prácticas de gestión de servicios de ITIL
- Estrategia de servicio
- Diseño de servicios
- Transición del servicio
- Funcionamiento del servicio
- Mejora continua del servicio.

Una estructura común en todas las publicaciones de orientación básica ayuda a encontrar fácilmente las referencias entre los volúmenes y dónde buscar temas de orientación similares dentro de cada etapa del ciclo de vida: [ITILv3]

Fundamentos de la práctica

Esta sección de cada publicación básica expone el argumento empresarial de la necesidad de considerar la gestión de servicios en un contexto de ciclo de vida y una visión general de las prácticas de esa etapa del ciclo de vida que contribuyen a ello. Se describe brevemente el contexto de las prácticas que siguen y cómo contribuyen al valor del negocio. [ITILv3]

Principios prácticos

Los principios de la práctica son las políticas y los aspectos de gobierno de esa etapa del ciclo de vida que anclan los procesos y las actividades tácticas para lograr sus objetivos. [ITILv3]

Procesos y actividades del ciclo de vida

Las etapas del ciclo de vida del servicio se basan en procesos para ejecutar cada elemento de la práctica de forma coherente, medible y repetible. Cada publicación central identifica los procesos que utiliza, cómo se integran con las otras etapas del ciclo de vida, y las actividades necesarias para llevarlas a cabo. [ITILv3]

Estructuras y funciones de la organización de apoyo

Cada publicación identifica las funciones y responsabilidades organizativas que deben considerarse para gestionar el ciclo de vida del servicio. Estos roles se proporcionan como una guía y pueden ser combinados para encajar en una variedad de estructuras organizativas. También se ofrecen sugerencias para estructuras organizativas óptimas. [ITILv3]

Consideraciones tecnológicas

Las prácticas de gestión de servicios de ITIL cobran impulso cuando se aplica el tipo adecuado de automatización técnica. Cada publicación del ciclo de vida hace recomendaciones sobre las áreas en las que se debe centrar la automatización tecnológica y los requisitos básicos que un proveedor de servicios querrá tener en cuenta al elegir las herramientas de gestión de servicios. [ITILv3]

Aplicación de la práctica

Para las organizaciones que son nuevas en ITIL, o las que desean mejorar la madurez de su práctica y su capacidad de servicio, cada publicación describe las mejores formas de implementar la etapa del ciclo de vida del servicio de ITIL. [ITILv3]

Desafíos, riesgos y factores críticos de éxito Siempre están presentes en cualquier organización. Cada publicación destaca los desafíos, riesgos y factores de éxito comunes que la mayoría de las organizaciones experimentan y cómo superarlos. [ITILv3]

Orientación complementaria

Hay muchos métodos, prácticas y marcos externos que se alinean bien con las prácticas de ITIL. Cada publicación ofrece una lista de ellos y de cómo se integran en el Ciclo de Vida del Servicio ITIL, cuándo son útiles y cómo. [ITILv3]

Ejemplos y plantillas

Cada publicación proporciona plantillas de trabajo y ejemplos de cómo se pueden aplicar las prácticas. Se ofrecen para ayudarle a aprovechar la experiencia y los conocimientos del sector que ya se utilizan. Cada una puede ser adaptada dentro de su contexto organizativo particular. [ITILv3]

33.11 Temas básicos de orientación - Estrategia de servicio

El núcleo del ciclo de vida del servicio es la estrategia del servicio. [ITILv3]

La Estrategia del Servicio proporciona orientación sobre cómo ver la gestión del servicio no sólo como una capacidad organizativa, sino como un activo estratégico. Se ofrece orientación sobre los principios en los que se basa la práctica de la gestión del servicio, que son útiles para desarrollar políticas, directrices y procesos de gestión del servicio a lo largo del ciclo de vida del servicio de ITIL. [ITILv3]

Los temas tratados en la Estrategia de Servicios incluyen el desarrollo de los mercados de servicios, las características de los tipos de proveedores internos y externos, los activos de servicios, la cartera de servicios y la aplicación de la estrategia a través del Ciclo de Vida de los Servicios. La Gestión Financiera, la Gestión de la Demanda, el Desarrollo Organizativo y los Riesgos Estratégicos son otros de los temas principales. [ITILv3]

Las organizaciones deben utilizar la orientación de la Estrategia de Servicios para establecer objetivos y expectativas de rendimiento para atender a los clientes y los espacios del mercado, y para identificar, seleccionar y priorizar las oportunidades. La Estrategia del Servicio consiste en asegurar que las organizaciones están en posición de manejar los costos y riesgos asociados a sus carteras de servicios y están preparadas no sólo para la eficacia operativa sino para un rendimiento distintivo. [ITILv3]

Las organizaciones que ya practican ITIL utilizan la Estrategia del Servicio para guiar una revisión estratégica de sus capacidades de gestión de servicios basadas en ITIL y para mejorar la alineación entre esas capacidades y sus estrategias de negocio. Este volumen de ITIL anima a los lectores a pararse a pensar por qué hay que hacer algo antes de pensar en el cómo. [ITILv3]

33.12 Temas básicos de Orientación - Diseño de servicios

Si lo construyes, vendrán" es un dicho de una famosa película de Hollywood de 1989, Campo de Sueños. Pero si lo construyes y no aporta valor, ¡pronto se irán! [ITILv3]

Para que los servicios aporten un verdadero valor a la empresa, deben diseñarse teniendo en cuenta los objetivos empresariales. El diseño del servicio es la etapa del ciclo de vida que convierte la estrategia del servicio en el proyecto para alcanzar los objetivos del negocio. [ITILv3]

El diseño de servicios proporciona orientación para el diseño y el desarrollo de servicios y prácticas de gestión de servicios. Abarca los principios y métodos de diseño para convertir los objetivos estratégicos en carteras de servicios y activos de servicios. El alcance del diseño de servicios no se limita a los nuevos servicios. Incluye los cambios y mejoras necesarios para aumentar o mantener el valor para los clientes durante el ciclo de vida de los servicios, la continuidad de los servicios, la consecución de los niveles de servicio y la conformidad con las normas y reglamentos. Orienta a las organizaciones sobre cómo desarrollar capacidades de diseño para la gestión de servicios. [ITILv3]

Entre los temas clave del Diseño del Servicio están el Catálogo de Servicios, la Disponibilidad, la Capacidad, la Continuidad y la Gestión del Nivel de Servicio. [ITILv3]

33.13 Temas básicos de Orientación - Transición de Servicios

Transición - Movimiento, paso o cambio de una posición, estado, etapa, tema, concepto, etc., a otro; cambio: la transición de la adolescencia a la edad adulta. [ITILv3]

La Transición del Servicio proporciona orientación para el desarrollo y la mejora de las capacidades para la transición de los servicios nuevos y modificados a la operación del servicio en vivo. Esta publicación proporciona orientación sobre cómo los requisitos de la Estrategia del Servicio codificados en el Diseño del Servicio se realizan efectivamente en la Operación del Servicio mientras se controlan los riesgos de fracaso e interrupción. [ITILv3]

La Transición de Servicios combina prácticas de Gestión de Cambios, Configuración, Activos, Lanzamiento y Despliegue, Programas y Riesgos y las sitúa en el contexto práctico de la gestión de servicios. Proporciona orientación sobre la gestión de la complejidad relacionada con los cambios en los servicios y los procesos de gestión de servicios, evitando consecuencias no deseadas y permitiendo al mismo tiempo la innovación. Se ofrece orientación sobre la transferencia del control de los servicios entre los clientes y los proveedores de servicios. [ITILv3]

La Transición del Servicio introduce el Sistema de Gestión del Conocimiento del Servicio, que se basa en los datos e información actuales dentro de los sistemas de Configuración, Capacidad, Errores Conocidos, Medios Definitivos y Activos, y amplía el uso de la información del servicio en la capacidad de conocimiento para la decisión y la gestión de los servicios. [ITILv3]

33.14 Temas básicos de Orientación - Funcionamiento del Servicio

El funcionamiento de los servicios engloba las prácticas de gestión del funcionamiento cotidiano de los servicios. Incluye orientación para lograr la eficacia y la eficiencia en la prestación y el apoyo de los servicios para garantizar el valor para el cliente y el proveedor de servicios. Los objetivos estratégicos se realizan en última instancia a través de la Operación del Servicio, por lo que es una capacidad crítica. Se ofrece orientación sobre cómo mantener la estabilidad en las operaciones de servicio, permitiendo cambios en el diseño, la escala, el alcance y los niveles de servicio. Las organizaciones reciben directrices detalladas sobre los procesos, métodos y herramientas para su uso en dos perspectivas principales de control: reactiva y proactiva. Los gestores y profesionales reciben conocimientos que les permiten tomar mejores decisiones en áreas como la gestión de la disponibilidad de los servicios, el control de la demanda, la optimización de la utilización de la capacidad, la programación de las operaciones y la solución de problemas. Se ofrece orientación sobre el apoyo a las operaciones a través de nuevos modelos y arquitecturas como los servicios compartidos, la informática de servicios públicos, los servicios web y el comercio móvil. [ITILv3]

Entre los temas que se presentan en este Service Operations están las prácticas de gestión de eventos, incidentes, problemas, solicitudes, aplicaciones y técnicas. En este libro se discuten algunas de las prácticas más recientes de la industria para gestionar arquitecturas virtuales y orientadas a servicios. [ITILv3]

33.15 Temas Básicos de Orientación - Mejora Continua del Servicio

La Mejora Continua de los Servicios proporciona una orientación instrumental para crear y mantener el valor para los clientes a través de un mejor diseño, transición y funcionamiento de los servicios. Combina principios, prácticas y métodos de la gestión de la calidad, la gestión del cambio y la mejora de la capacidad. Las organizaciones aprenden a realizar mejoras incrementales y a gran escala en la calidad del servicio, la eficiencia operativa y la continuidad del negocio. Se ofrece orientación para vincular los esfuerzos de mejora y los resultados con la estrategia, el diseño y la transición de los servicios. Se establece un sistema de retroalimentación de bucle cerrado, basado en el modelo Deming Plan-Do-Check-Act (PDCA), capaz de recibir aportaciones para las mejoras desde cualquier perspectiva de planificación. [ITILv3]

Entre los temas clave se encuentra la orientación sobre la medición del servicio, la demostración del valor con métricas, el desarrollo de líneas de base y las evaluaciones de madurez. [ITILv3]

34 Apéndice C - Instituto Nacional de Ciencia y Tecnología

El Instituto Nacional de Ciencia y Tecnología (NIST) promulga normas de ciberseguridad para su uso por parte de los organismos del gobierno federal y otros que deseen operar de forma segura los sistemas de información y los sistemas de control industrial (ICS).

La versión actual de las normas de ciberseguridad del NIST puede encontrarse aquí: https://csrc.nist.gov/publications/final-pubs

35 Apéndice D - Sistemas de Información de la Justicia Penal (CJIS)

Los Sistemas de Información de Justicia Penal (CJIS) son una red de sistemas de aplicación de la ley, gestionados a nivel nacional por la Oficina Federal de Investigación (FBI). En el funcionamiento del CJIS, el FBI trabaja en colaboración con los gobiernos estatales, locales y tribales para compartir información relacionada con la justicia penal y publica las normas que deben cumplir los organismos encargados de hacer cumplir la ley para la gestión y el almacenamiento de la información sobre justicia penal (CJI). [FBI]

La premisa esencial de la Política de Seguridad CJIS es proporcionar los controles adecuados para proteger el ciclo de vida completo de la ICJ, ya sea en reposo o en tránsito. La política de seguridad del CJIS proporciona orientación para la creación, visualización, modificación, transmisión, difusión, almacenamiento y destrucción de la ICJ. [Política de seguridad del CJIS]

La Ciudad de Dallas, al gestionar los datos de CJIS, está obligada a cumplir con las políticas y normas federales y estatales que rigen CJIS. Como se ha dicho anteriormente, el FBI mantiene su Política de Seguridad CJIS federal, mientras que el Departamento de Seguridad Pública de Texas (DPS) publica un Documento de Acompañamiento de Requisitos y una Política de Seguridad CJIS de Texas que acompaña a la Política de Seguridad CJIS del FBI. El DPS de Texas también es responsable de auditar el cumplimiento de los municipios con los requisitos federales y estatales del CJIS.

La política federal de seguridad del CJIS exige que los organismos desarrollen, difundan y mantengan procedimientos formales y documentados para facilitar la aplicación de la política de seguridad del CJIS y, en su caso, de la política de seguridad local. Las políticas y procedimientos deberán ser coherentes con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos, normas y orientaciones aplicables. Los procedimientos desarrollados para las áreas de la Política de Seguridad CJIS pueden ser desarrollados para el programa de seguridad en general, y para un sistema de información en particular, cuando sea necesario. [Política Federal de Seguridad CJIS]

La política de seguridad del CJIS contempla los datos (información), los servicios y los controles de protección que se aplican independientemente de la arquitectura de implementación. La independencia de la arquitectura no pretende disminuir la importancia de los sistemas, sino prever la sustitución de una tecnología por otra, garantizando al mismo tiempo que los controles necesarios para proteger la información permanezcan constantes. [Política Federal de Seguridad del CJIS]

El objetivo y el enfoque conceptual de la Política de Seguridad CJIS en los ámbitos de la política de seguridad proporcionan la orientación y las normas, al tiempo que evitan el impacto del panorama en constante cambio de las innovaciones técnicas. La independencia arquitectónica de la Política proporciona a los organismos la flexibilidad necesaria para ajustar su infraestructura y sus políticas de seguridad de la información para reflejar sus propios entornos. [Política Federal de Seguridad CJIS]

La política de seguridad del CJIS define los tipos de información que componen la CJI. Se incluye en esta categoría:

- Datos biométricos,
- Datos del historial de identidad,
- Datos biográficos,
- Datos de la propiedad, y
- Historial de casos o incidentes. [Política Federal de Seguridad del CJIS]

El DPS de Texas adopta la Política de Seguridad CJIS federal como la política de seguridad para el Estado de Texas, pero también publica la Política de Seguridad CJIS de Texas. En consonancia con la CSP y además de ella, el DPS requiere que cada agencia se adhiera a las siguientes normas, que deberán ser seguidas por todas las agencias que acceden a los datos de Justicia Penal en el Estado de Texas:

1. Actualizaciones del sistema - Todos los componentes de los sistemas de TI con conectividad al CJIS se actualizarán con todas las correcciones, actualizaciones y parches de seguridad disponibles en un plazo de 30 días a partir de su disponibilidad. Esto se aplica a las estaciones de trabajo, los servidores, los ordenadores portátiles, los conmutadores, los enrutadores y todos los demás equipos informáticos gestionados.
2. Equipos al final de su vida útil - Todos los sistemas informáticos con conectividad al CJIS deberán ser sustituidos en un plazo de 6 meses desde que lleguen al "final de su vida útil", o desde que dejen de recibir el apoyo del fabricante con correcciones, actualizaciones y parches de seguridad.
3. Ubicación físicamente segura - Una ubicación físicamente segura es una instalación, un vehículo policial cerrado, o un área, una sala o un grupo de salas dentro de una instalación con los

controles de seguridad tanto físicos como de personal suficientes para proteger la ICJ y los sistemas de información asociados.

4. Controles compensatorios para la autenticación avanzada - Se permiten los controles compensatorios aprobados por el Director de Seguridad para cumplir con el requisito de autenticación avanzada en los teléfonos inteligentes y tabletas emitidos por la agencia con sistemas operativos de características limitadas. Los controles compensatorios son medidas de control temporales que se implementan en lugar de las medidas de control de autenticación avanzada requeridas cuando una agencia no puede cumplir con un requisito debido a limitaciones técnicas o comerciales legítimas. [Política de seguridad del CJIS de Texas]

Por último, el documento complementario de los requisitos del DPS de Texas, que describe los cambios realizados en las políticas. El Texas DPS Requirements Companion Document proporciona orientación sobre los cambios de política, qué actor es responsable de garantizar la aplicación de la política, y la priorización de la aplicación de los cambios de política. [Documento de acompañamiento de los requisitos del DPS de Texas]

36 Términos Generales y Acrónimos

AD - Dirección Administrativa (documento de política interna) o Director Adjunto (cargo/función)

Datos de archivo: datos históricos que se conservan por razones de retención a largo plazo. El apoyo al cumplimiento es una de las razones por las que estos datos pueden estar sujetos a reglas de negocio de retención a largo plazo.

BABOK - Business Analyst Body of Knowledge

Datos de copia de seguridad: datos actuales o recientes que se mantienen para restaurar los datos operativos de los sistemas de información en caso de una interrupción del servicio o de un incidente de servicio relacionado con los datos operativos.

CIO - Director de Información

CISO - Director de Seguridad de la Información

CJIS - Sistema de Información de la Justicia Penal

DAMA - Gestión de datos (DAMA) Internacional

DMBOK - Conjunto de conocimientos sobre gestión de datos

DHS - El Departamento de Seguridad Nacional

DOJ - El Departamento de Justicia

DPS - Departamento de Seguridad Pública (generalmente se refiere al Departamento de Seguridad Pública del Estado de Texas)

FBI - Oficina Federal de Investigación

GB - Gigabyte

HIPAA - Ley de Portabilidad y Responsabilidad del Seguro Médico

IAM - Gestión de identidades y accesos

Tecnología de la información

ITIL - Biblioteca de Infraestructura de Tecnologías de la Información

NIST - Instituto Nacional de Normas y Tecnología

PMBOK - Cuerpo de conocimientos de gestión de proyectos

TB - Terabyte

37 Acrónimos de Gestión de Servicios de TI

BC - Continuidad de negocio

DR - Recuperación de desastres

IAM - Gestión de identidades y accesos

ITBC - Continuidad del negocio de TI

ITIL - Biblioteca de Infraestructura de Tecnologías de la Información

38 Solución Acrónimos

AMS - American Management Solutions (se refiere a la solución de contabilidad gubernamental CGI Advantage)

CAD - Computer Aided Dispatch (utilizado por los elementos de seguridad pública de la Ciudad)

CAPERS - Delitos contra las personas

SIG - Sistema de Información Geográfica

RMS - Sistema de gestión de registros

39 Códigos/Acrónimos de los Departamentos

ATT - Oficina del Fiscal de la Ciudad

AUD - Oficina del Auditor de la Ciudad

AVI - Departamento de Aviación

CIS - Departamento de Comunicaciones y Servicios de Información (antigua denominación de ITS)

DFR - Bomberos de Dallas

DPD - Departamento de Policía de Dallas

DSV - Servicios de datos (código contable para ITS)

DWU - Servicios de agua de Dallas

ITS - Departamento de Servicios de Información y Tecnología

PBW - Departamento de Obras Públicas

PKR - Departamento de Parques y Actividades Recreativas

40 Glosario (Términos de Interés de ITILv3)

Gestor de cuentas - Función muy similar a la de gestor de relaciones comerciales, pero que incluye más aspectos comerciales. Se utiliza sobre todo cuando se trata de clientes externos.

Aplicación - Software que proporciona Funciones que son requeridas por un Servicio de TI. Cada aplicación puede formar parte de más de un servicio de TI. Una aplicación se ejecuta en uno o más servidores o clientes. Véase también Gestión de aplicaciones.

Gestión de aplicaciones - Función responsable de la gestión de las aplicaciones a lo largo de su ciclo de vida.

Ensamblaje - Un elemento de configuración (CI) que se compone de una serie de otros CIs. Por ejemplo, un CI de servidor puede contener CIs para CPUs, discos, memoria, etc.; un CI de servicio de TI puede contener muchos CIs de hardware, software y otros. Véase también Build.

Evaluación - Inspección y análisis para comprobar si se cumple una norma o conjunto de directrices, si los registros son precisos o si se cumplen los objetivos de eficiencia y eficacia. Véase también Auditoría.

Activo - Cualquier recurso o capacidad. Los activos de un proveedor de servicios incluyen cualquier cosa que pueda contribuir a la prestación de un servicio. Los activos pueden ser de uno de los siguientes tipos: Gestión, Organización, Proceso, Conocimiento, Personas, Información, Aplicaciones, Infraestructura y Capital Financiero.

Gestión de Activos - La Gestión de Activos es el Proceso responsable de rastrear y reportar el valor y la propiedad de los Activos financieros a lo largo de su Ciclo de Vida. La Gestión de Activos forma parte de un Proceso global de Gestión de Activos de Servicio y Configuración. Véase también Registro de Activos.

Registro de Activos - Una lista de Activos que incluye su propiedad y valor. La Gestión de Activos mantiene el Registro de Activos.

Auditoría - Inspección y verificación formal para comprobar si se cumple una norma o conjunto de directrices, si los registros son exactos o si se cumplen los objetivos de eficiencia y eficacia. Una auditoría puede ser realizada por grupos internos o externos. Véase también Certificación, Evaluación.

Disponibilidad - Capacidad de un elemento de configuración o servicio de TI para realizar su función acordada cuando se requiera. La disponibilidad está determinada por la fiabilidad, la capacidad de mantenimiento, la capacidad de servicio, el rendimiento y la seguridad. La disponibilidad suele calcularse en forma de porcentaje. Este cálculo suele basarse en el tiempo de servicio acordado y en el tiempo de inactividad. Es una Buena Práctica calcular la Disponibilidad usando mediciones de los resultados del Negocio del Servicio de TI.

Gestión de la Disponibilidad - Proceso responsable de definir, analizar, planificar, medir y mejorar todos los aspectos de la disponibilidad de los servicios de TI. La Gestión de la Disponibilidad es responsable de garantizar que toda la Infraestructura de TI, los Procesos, las Herramientas, los Roles, etc. sean apropiados para los Objetivos de Nivel de Servicio acordados para la Disponibilidad.

Back-out - Recuperación a un estado conocido después de un cambio o liberación fallida.

Plan de respaldo - Un plan para recuperar un servicio a un estado conocido después de un Cambio o Liberación fallido.

Copia de seguridad - Copia de datos para protegerlos contra la pérdida de integridad o disponibilidad del original.

Mejor práctica - Actividades o procesos probados que han sido utilizados con éxito por múltiples organizaciones. ITIL es un ejemplo de Mejor Práctica.

Construcción - Actividad de ensamblar una serie de elementos de configuración para crear parte de un servicio de TI. El término Build también se utiliza para referirse a una versión autorizada para su distribución. Por ejemplo, Build de servidor o Build de portátil.

Entorno de construcción - Entorno controlado en el que se ensamblan las aplicaciones, los servicios de TI y otras construcciones antes de trasladarlos a un entorno de prueba o en vivo.

Negocio - (Estrategia de Servicio) Una entidad corporativa global u Organización formada por un número de Unidades de Negocio. En el contexto de ITSM, el término Negocio incluye organizaciones del sector público y sin ánimo de lucro, así como empresas. Un proveedor de servicios de TI proporciona servicios de TI a un cliente dentro de una empresa. El Proveedor de Servicios TI puede formar parte de la misma

Empresa que su Cliente (Proveedor de Servicios Interno), o formar parte de otra Empresa (Proveedor de Servicios Externo).

Caso de negocio - (Estrategia de servicio) Justificación de un gasto importante. Incluye información sobre costos, beneficios, opciones, cuestiones, riesgos y posibles problemas.

Plan de Continuidad de Negocio (BCP) - (Diseño del Servicio) Un plan que define los pasos necesarios para restaurar los procesos de negocio tras una interrupción. El Plan también identificará los desencadenantes de la invocación, las personas que deben participar, las comunicaciones, etc. Los Planes de Continuidad del Servicio de TI constituyen una parte importante de los Planes de Continuidad del Negocio.

Cliente de la empresa - Un destinatario de un producto o un servicio de la empresa. Por ejemplo, si la empresa es un fabricante de coches, el cliente comercial es alguien que compra un coche.

Objetivo de negocio - El objetivo de un proceso de negocio, o del negocio en su conjunto. Los Objetivos de Negocio apoyan la Visión de Negocio, proporcionan una guía para la Estrategia de TI, y a menudo son apoyados por los Servicios de TI.

Operaciones de negocio - La ejecución diaria, el seguimiento y la gestión de los procesos de negocio.

Proceso de Negocio - Un Proceso que es propiedad de la Empresa y que es llevado a cabo por la misma. Un proceso empresarial contribuye a la entrega de un producto o servicio a un cliente empresarial. Por ejemplo, un minorista puede tener un Proceso de compra que ayuda a entregar Servicios a sus Clientes de Negocio. Muchos Procesos de Negocio dependen de los Servicios de TI.

Gestión de las Relaciones con la Empresa - Proceso o función responsable de mantener una relación con la empresa. La gestión de las relaciones comerciales suele incluir:

- Gestión de las relaciones personales con los directivos de las empresas
- Aportación a la gestión de la cartera de servicios
- Garantía de que el proveedor de servicios de TI satisface las necesidades empresariales de los clientes.

Este proceso está estrechamente relacionado con la gestión del nivel de servicio.

Servicio de Negocio - Un Servicio de TI que soporta directamente un Proceso de Negocio, a diferencia de un Servicio de Infraestructura, que es utilizado internamente por el Proveedor de Servicios de TI y no suele ser visible para el Negocio.

El término "servicio empresarial" también se utiliza para referirse a un servicio prestado a clientes empresariales por unidades de negocio. Por ejemplo, la entrega de servicios financieros a los clientes de un banco, o de bienes a los clientes de una tienda minorista. El éxito de la prestación de los Servicios de Negocio depende a menudo de uno o más Servicios de TI.

Gestión de Servicios de Negocio (BSM) - Un enfoque de la gestión de los Servicios de TI que considera los Procesos de Negocio soportados y el valor de Negocio proporcionado. Este término también se refiere a la gestión de los servicios empresariales prestados a los clientes empresariales.

Disco de Negocio - Un segmento del negocio que tiene sus propios planes, métricas, ingresos y costos. Cada Disco de Negocio posee Activos y los utiliza para crear valor para los Clientes en forma de bienes y Servicios.

Capacidad - La habilidad de una Organización, persona, Proceso, Aplicación, Elemento de Configuración o Servicio de TI para llevar a cabo una Actividad. Las capacidades son Activos intangibles de una Organización. Véase también Recurso.

Capacidad - El máximo rendimiento que un elemento de configuración o servicio de TI puede ofrecer cumpliendo los objetivos de nivel de servicio acordados. Para algunos tipos de CI, la capacidad puede ser el tamaño o el volumen, por ejemplo, una unidad de disco.

Gestión de la capacidad: proceso responsable de garantizar que la capacidad de los servicios de TI y la infraestructura de TI puedan cumplir los objetivos de nivel de servicio acordados de forma rentable y oportuna. La gestión de la capacidad tiene en cuenta todos los recursos necesarios para prestar el servicio de TI y planifica los requisitos empresariales a corto, medio y largo plazo.

Plan de capacidad - El plan de capacidad se utiliza para gestionar los recursos necesarios para prestar los servicios de TI. El plan contiene escenarios para diferentes predicciones de la demanda de la empresa y opciones con costos para cumplir los objetivos de nivel de servicio acordados.

Categoría - Grupo de cosas que tienen algo en común. Las categorías se utilizan para agrupar cosas similares. Por ejemplo, los tipos de costos se utilizan para agrupar tipos similares de costos, las categorías de incidentes se utilizan para agrupar tipos similares de incidentes, los tipos de CI se utilizan para agrupar tipos similares de elementos de configuración.

Cambio - La adición, modificación o eliminación de cualquier cosa que pueda tener un efecto en los Servicios de TI. El alcance debe incluir todos los servicios de TI, elementos de configuración, procesos, documentación, etc.

Junta Consultiva de Cambios (CAB) - Un grupo de personas que asesora al Gestor de Cambios en la Evaluación, priorización y programación de los Cambios. Esta junta suele estar formada por representantes de todas las áreas del proveedor de servicios de TI, representantes de la empresa y terceros, como los proveedores.

Historial de Cambios - Información sobre todos los cambios realizados a un Elemento de Configuración durante su vida. El Historial de Cambios consiste en todos aquellos Registros de Cambios que se aplican al CI.

Gestión de cambios - Proceso responsable de controlar el ciclo de vida de todos los cambios. El objetivo principal de la Gestión de Cambios es permitir que se realicen cambios beneficiosos, con una interrupción mínima de los servicios de TI.

Modelo de cambio - Una forma repetible de tratar una categoría de cambio en particular. Un modelo de cambio define los pasos específicos predefinidos que se seguirán para un cambio de esta categoría. Los modelos de cambio pueden ser muy sencillos, sin necesidad de aprobación (por ejemplo, el restablecimiento de la contraseña) o pueden ser muy complejos, con muchos pasos que requieren aprobación (por ejemplo, un lanzamiento importante de software). Véase también Cambio estándar, Junta Consultiva de Cambios.

Registro de cambios - Un registro que contiene los detalles de un cambio. Cada registro de cambio documenta el ciclo de vida de un solo cambio. Se crea un registro de cambio para cada solicitud de cambio que se recibe, incluso para las que se rechazan posteriormente. Los registros de cambios deben hacer referencia a los elementos de configuración afectados por el cambio. Los registros de cambio se almacenan en el sistema de gestión de la configuración.

Solicitud de cambio - Véase Solicitud de cambio.

Cronograma de Cambios - Documento que enumera todos los Cambios aprobados y sus fechas de implementación previstas. Un Calendario de Cambios se denomina a veces Calendario de Cambios Futuro, aunque también contiene información sobre los Cambios que ya se han implementado.

Ventana de cambio - Un tiempo regular y acordado en el que los cambios o lanzamientos pueden ser implementados con un impacto mínimo en los servicios. Las ventanas de cambio suelen estar documentadas en los SLA.

Tipo de CI - Una categoría que se utiliza para clasificar los CIs. El Tipo de CI identifica los Atributos y Relaciones requeridos para un Registro de Configuración. Los tipos de CI más comunes son: Hardware, Documento, Usuario, etc.

Clasificación - El acto de asignar una categoría a algo. La clasificación se utiliza para garantizar la coherencia de la gestión y de los informes. Normalmente se clasifican los CI, los incidentes, los problemas, los cambios, etc.

Cliente - Término genérico que designa a un cliente, a la empresa o a un cliente empresarial. Por ejemplo, gestor de clientes puede utilizarse como sinónimo de gestor de cuentas. El término cliente también se utiliza para significar:

- Un ordenador que es utilizado directamente por un usuario, por ejemplo un PC, un ordenador de mano o una estación de trabajo
- La parte de una aplicación cliente-servidor con la que el usuario interactúa directamente. Por ejemplo, un cliente de correo electrónico.

Cerrado - El estado final en el ciclo de vida de un incidente, problema, cambio, etc. Cuando el estado es Cerrado, no se realizan más acciones.

Cierre - El acto de cambiar el estado de un incidente, problema, cambio, etc. ha cerrado.

Cumplimiento - Garantizar que se sigue una norma o conjunto de directrices, o que se emplean prácticas contables u otras adecuadas y coherentes.

Componente - Término general que se utiliza para referirse a una parte de algo más complejo. Por ejemplo, un Sistema informático puede ser un componente de un Servicio de TI, una Aplicación puede ser un Componente de una Disco de Liberación. Los componentes que deben ser gestionados deben ser Elementos de Configuración.

Configuración - Término genérico, utilizado para describir un grupo de Elementos de Configuración que trabajan juntos para entregar un Servicio de TI, o una parte reconocible de un Servicio de TI. La configuración también se utiliza para describir los ajustes de los parámetros de uno o más CIs.

Elemento de configuración (CI): cualquier componente que deba gestionarse para prestar un servicio de TI. La información sobre cada CI se registra en un Registro de Configuración dentro del Sistema de Gestión de la Configuración y se mantiene a lo largo de su Ciclo de Vida por la Gestión de la Configuración. Los CIs están bajo el control de la Gestión de Cambios. Los CIs suelen incluir Servicios de TI, hardware, software, edificios, personas y documentación formal como la documentación de Procesos y los SLAs.

Gestión de la Configuración - Proceso responsable de mantener la información sobre los Elementos de Configuración necesarios para prestar un Servicio de TI, incluyendo sus Relaciones. Esta información se gestiona a lo largo del Ciclo de Vida del CI. La Gestión de la Configuración es parte de un Proceso de Gestión de Activos y Configuración del Servicio en general.

Base de datos de gestión de la configuración (CMDB): base de datos utilizada para almacenar los registros de configuración a lo largo de su ciclo de vida. El Sistema de Gestión de la Configuración mantiene una o más CMDBs, y cada CMDB almacena Atributos de CIs, y Relaciones con otros CIs.

Sistema de gestión de la configuración (CMS) - Conjunto de herramientas y bases de datos que se utilizan para gestionar los datos de configuración de un proveedor de servicios de TI. El CMS también incluye información sobre Incidentes, Problemas, Errores Conocidos, Cambios y Liberaciones; y puede contener datos sobre empleados, Proveedores, ubicaciones, Unidades de Negocio, Clientes y Usuarios. El CMS incluye herramientas para recoger, almacenar, gestionar, actualizar y presentar datos sobre todos los elementos de configuración y sus relaciones. El CMS es mantenido por la Gestión de la Configuración y es utilizado por todos los Procesos de Gestión de Servicios de TI. Véase también Base de Datos de Gestión de la Configuración, Sistema de Gestión del Conocimiento del Servicio.

Registro de configuración - Registro que contiene los detalles de un elemento de configuración. Cada registro de configuración documenta el ciclo de vida de un solo CI. Los registros de configuración se almacenan en una base de datos de gestión de la configuración.

Estructura de la configuración - La jerarquía y otras relaciones entre todos los elementos de configuración que componen una configuración.

Mejora Continua del Servicio (CSI) - Una etapa del Ciclo de Vida de un Servicio de TI y el título de una de las publicaciones principales de ITIL. La Mejora Continua del Servicio se encarga de gestionar las mejoras de los Procesos de Gestión del Servicio de TI y de los Servicios de TI. El rendimiento del proveedor de servicios de TI se mide continuamente y se realizan mejoras en los procesos, los servicios de TI y la infraestructura de TI con el fin de aumentar la eficiencia, la eficacia y la rentabilidad. Véase también Planificar-Hacer-Verificar-Actuar.

Control - Un medio para gestionar un riesgo, garantizar que se logre un objetivo empresarial o asegurar que se siga un proceso. Algunos ejemplos de controles son las políticas, los procedimientos, las funciones, el RAID, los cierres de puertas, etc. Un control se denomina a veces contramedida o salvaguarda. Controlar también significa gestionar la utilización o el comportamiento de un elemento de configuración, sistema o servicio de TI.

Perspectiva de Control - Un enfoque para la gestión de los Servicios de TI, Procesos, Funciones, Activos, etc. Puede haber varias Perspectivas de Control diferentes en el mismo Servicio de TI, Proceso, etc., permitiendo a diferentes individuos o equipos centrarse en lo que es importante y relevante para su Rol específico. Ejemplos de Perspectivas de Control incluyen la gestión Reactiva y Proactiva dentro de las Operaciones de TI, o una vista del Ciclo de Vida para un equipo de Proyecto de Aplicación.

Costo - La cantidad de dinero que se gasta en una actividad específica, un servicio de TI o una disco de negocio. Los costos consisten en un costo real (dinero), un costo nocional, como el tiempo de las personas, y la depreciación.

Rentabilidad - Medida del equilibrio entre la eficacia y el costo de un servicio, proceso o actividad. Un proceso rentable es aquel que logra sus objetivos con un costo mínimo. Véase también KPI, Retorno de la Inversión, Valor por Dinero.

Contramedida - Puede utilizarse para referirse a cualquier tipo de control. El término contramedida se utiliza con mayor frecuencia cuando se refiere a medidas que aumentan la resiliencia, la tolerancia a los fallos o la fiabilidad de un servicio de TI.

Gestión de crisis - La gestión de crisis es el proceso responsable de gestionar las implicaciones más amplias de la continuidad del negocio. Un equipo de gestión de crisis es responsable de cuestiones estratégicas como la gestión de las relaciones con los medios de comunicación y la confianza de los accionistas, y decide cuándo invocar los planes de continuidad de la actividad.

Factor Crítico de Éxito (CSF) - Algo que debe ocurrir para que un Proceso, Proyecto, Plan o Servicio de TI tenga éxito. Los KPIs se utilizan para medir la consecución de cada CSF. Por ejemplo, un CSF de "proteger los Servicios de TI al hacer Cambios" podría ser medido por KPIs como "porcentaje de reducción de Cambios no exitosos", "porcentaje de reducción de Cambios que causan Incidentes", etc.

Cultura - Conjunto de valores que comparte un grupo de personas, incluidas las expectativas sobre cómo deben comportarse las personas, sus ideas, creencias y prácticas. Véase también Visión. Cliente Persona que compra bienes o servicios. El Cliente de un Proveedor de Servicios de TI es la persona o grupo que define y acuerda los Objetivos de Nivel de Servicio. El término Clientes también se utiliza a veces de manera informal para referirse a los Usuarios, por ejemplo "esta es una Organización centrada en el Cliente".

De los datos a la información, del conocimiento a la sabiduría (DIKW) - Una forma de entender las relaciones entre los datos, la información, el conocimiento y la sabiduría. DIKW muestra cómo cada uno de ellos se basa en los demás.

Mediateca definitiva (DML): una o varias ubicaciones en las que se almacenan de forma segura las versiones definitivas y aprobadas de todos los elementos de configuración del software. La LMD también puede contener los elementos de configuración asociados, como las licencias y la documentación. El LMD es una única área de almacenamiento lógico aunque haya varias ubicaciones. Todo el software de la LMD está bajo el control de la Gestión de Cambios y Liberaciones y se registra en el Sistema de Gestión de la Configuración. Sólo el software del LMD es aceptable para su uso en una versión.

Entregable - Algo que debe proporcionarse para cumplir un compromiso en un Acuerdo de Nivel de Servicio o un Contrato. Entregable también se utiliza de manera más informal para referirse a un resultado planificado de cualquier proceso.

Gestión de la demanda: actividades que comprenden e influyen en la demanda de servicios por parte de los clientes y en la provisión de capacidad para satisfacer dicha demanda. A nivel estratégico, la gestión de la demanda puede incluir el análisis de los patrones de actividad empresarial y los perfiles de los usuarios. A nivel táctico, puede implicar el uso de la tarificación diferencial para animar a los clientes a utilizar los servicios de TI en momentos de menor actividad. Véase también Gestión de la capacidad.

Diseño - Actividad o proceso que identifica los requisitos y luego define una solución capaz de satisfacer estos requisitos. Véase también Diseño de servicios.

Cambio de emergencia - Un cambio que debe introducirse lo antes posible. Por ejemplo, para resolver un incidente importante o implementar un parche de seguridad. El Proceso de Gestión de Cambios normalmente tendrá un Procedimiento específico para manejar los Cambios de Emergencia. Véase también Junta Consultiva de Cambios de Emergencia (ECAB).

Junta Consultiva de Cambios de Emergencia (ECAB) - Es un subgrupo de la Junta Consultiva de Cambios que toma decisiones sobre los cambios de emergencia de alto impacto. La composición de la ECAB puede decidirse en el momento de convocar una reunión y depende de la naturaleza del cambio de emergencia.

Entorno - Subconjunto de la infraestructura de TI que se utiliza para un fin determinado. Por ejemplo: Entorno activo, Entorno de prueba, Entorno de construcción. Es posible que varios entornos compartan un elemento de configuración, por ejemplo, los entornos de prueba y los activos pueden utilizar diferentes particiones en un único ordenador central. También se utiliza el término Entorno Físico para referirse al alojamiento, el aire acondicionado, el sistema de alimentación, etc.

Error - Una falla de diseño o un mal funcionamiento que causa una falla en uno o más elementos de configuración o servicios de TI. Un error cometido por una persona o un Proceso defectuoso que afecta a un IC o Servicio de TI también es un Error.

Evento - Un cambio de estado que tiene importancia para la gestión de un elemento de configuración o servicio de TI.

Fallo - Pérdida de la capacidad de operar de acuerdo con las especificaciones, o de entregar el resultado requerido. El término "fallo" puede utilizarse para referirse a servicios de TI, procesos, actividades, elementos de configuración, etc. Un fallo suele provocar un incidente.

Fallo - Ver Error.

Tolerancia a los fallos: capacidad de un servicio informático o de un elemento de configuración para seguir funcionando correctamente tras el fallo de un componente. Véase también Resiliencia, Contramedida.

Adecuación al propósito - Término informal utilizado para describir un proceso, elemento de configuración, servicio de TI, etc. que es capaz de cumplir sus objetivos o niveles de servicio. La adecuación al propósito requiere un diseño, una implementación, un control y un mantenimiento adecuados.

Cumplimiento - Realización de actividades para satisfacer una necesidad o requerimiento. Por ejemplo, proporcionando un nuevo servicio de TI o satisfaciendo una solicitud de servicio.

Gobernanza - Garantizar que las políticas y la estrategia se aplican realmente, y que los procesos requeridos se siguen correctamente. La gobernanza incluye la definición de funciones y responsabilidades, la medición y la presentación de informes, y la adopción de medidas para resolver los problemas detectados.

Integridad - Principio de seguridad que garantiza que los datos y los elementos de configuración sean modificados únicamente por el personal y las actividades autorizadas. La integridad tiene en cuenta todas las posibles causas de modificación, incluidos los fallos de software y hardware, los eventos ambientales y la intervención humana.

Infraestructura de TI - Todo el hardware, software, redes, instalaciones, etc. que se requieren para desarrollar, probar, entregar, supervisar, controlar o apoyar los servicios de TI. El término infraestructura de TI incluye toda la tecnología de la información, pero no las personas, los procesos y la documentación asociados.

Operaciones de TI - Actividades llevadas a cabo por el Control de Operaciones de TI, incluyendo la gestión de la consola, la programación de trabajos, la copia de seguridad y la restauración, y la gestión de la impresión y la salida. Operaciones de TI también se utiliza como sinónimo de Operación de Servicios.

Gestión de operaciones de TI: la función dentro de un proveedor de servicios de TI que realiza las actividades diarias necesarias para gestionar los servicios de TI y la infraestructura de TI de apoyo. La gestión de las operaciones de TI incluye el control de las operaciones de TI y la gestión de las instalaciones.

Servicio de TI - Servicio prestado a uno o más clientes por un proveedor de servicios de TI. Un Servicio de TI se basa en el uso de Tecnologías de la Información y apoya los Procesos de Negocio del Cliente. Un Servicio de TI se compone de una combinación de personas, Procesos y tecnología y debe ser definido en un Acuerdo de Nivel de Servicio.

Plan de continuidad del servicio de TI - Plan que define los pasos necesarios para recuperar uno o varios servicios de TI. El Plan también identificará los desencadenantes de la Invocación, las personas que deben participar, las comunicaciones, etc. El Plan de Continuidad del Servicio de TI debe formar parte de un Plan de Continuidad del Negocio.

Gestión de servicios de TI (ITSM) - La implementación y gestión de servicios de TI de calidad que satisfagan las necesidades del negocio. La gestión de los servicios de TI la realizan los proveedores de servicios de TI mediante una combinación adecuada de personas, procesos y tecnologías de la información. Véase también Gestión de Servicios.

ITIL - Un conjunto de orientaciones sobre las mejores prácticas para la gestión de servicios de TI. ITIL es propiedad de la Oficina de Comercio del Gobierno del Reino Unido y consiste en una serie de publicaciones que ofrecen orientación sobre la prestación de servicios de TI de calidad y sobre los procesos e instalaciones necesarios para apoyarlos. Para más información, consulte www.itil.co.uk.

Gestión del conocimiento - Proceso responsable de reunir, analizar, almacenar y compartir el conocimiento y la información dentro de una organización. El objetivo principal de la Gestión del Conocimiento es mejorar la eficiencia reduciendo la necesidad de redescubrir el conocimiento. Véase

también Datos-a-Información-a-Conocimiento-a-Sabiduría, Sistema de Gestión del Conocimiento de los Servicios.

Mantenibilidad - Medida de la rapidez y eficacia con la que un elemento de configuración o servicio de TI puede volver a funcionar normalmente después de un fallo. La mantenibilidad suele medirse y notificarse como MTRS. La capacidad de mantenimiento también se utiliza en el contexto del desarrollo de software o servicios de TI para referirse a la capacidad de cambiar o reparar fácilmente.

Incidente grave - La categoría más alta de impacto de un incidente. Un incidente grave provoca una perturbación importante en la empresa.

Información de gestión - Información que se utiliza para apoyar la toma de decisiones por parte de los gestores. La información de gestión suele ser generada automáticamente por las herramientas que apoyan los diversos procesos de gestión de servicios de TI. La información de gestión suele incluir los valores de los KPI, como el "porcentaje de cambios que dan lugar a incidentes" o la "tasa de reparación a la primera".

Sistema de gestión - El marco de políticas, procesos y funciones que garantiza que una organización pueda alcanzar sus objetivos.

Madurez - Una medida de la fiabilidad, eficiencia y eficacia de un proceso, función, organización, etc. Los procesos y funciones más maduros están formalmente alineados con los objetivos y la estrategia de la empresa y se apoyan en un marco de mejora continua.

Objetivo - La finalidad definida de un proceso, una actividad o una organización en su conjunto. Los objetivos suelen expresarse como metas medibles. El término Objetivo también se utiliza informalmente para referirse a un requisito. Véase también Resultado.

Operar - Funcionar como se espera. Se dice que un proceso o elemento de configuración funciona si proporciona los resultados requeridos. Operar también significa realizar una o más operaciones. Por ejemplo, hacer funcionar un ordenador es realizar las operaciones diarias necesarias para que funcione como se espera.

Operación - Gestión diaria de un servicio de TI, sistema u otro elemento de configuración. Operación también se utiliza para referirse a cualquier Actividad o Transacción predefinida. Por ejemplo, cargar una cinta magnética, aceptar dinero en un punto de venta o leer datos de una unidad de disco.

Operativo - El más bajo de los tres niveles de planificación y entrega (Estratégico, Táctico, Operativo). Las actividades operativas incluyen la planificación o entrega diaria o a corto plazo de un proceso de negocio o de un proceso de gestión de servicios de TI. El término Operativo es también un sinónimo de Vivo.

Acuerdo de Nivel Operativo (OLA) - Acuerdo entre un Proveedor de Servicios de TI y otra parte de la misma Organización. Un OLA respalda la prestación de Servicios de TI a los Clientes por parte del Proveedor de Servicios de TI. El OLA define los bienes o servicios que se van a prestar y las responsabilidades de ambas partes. Por ejemplo, podría haber un OLA:

- Entre el proveedor de servicios informáticos y un departamento de compras para obtener el hardware en los plazos acordados
- Entre el Service Desk y un grupo de soporte para proporcionar la resolución de incidentes en los tiempos acordados. Véase también Acuerdo de Nivel de Servicio.

Resultado - Resultado de la realización de una actividad, de un proceso, de la prestación de un servicio informático, etc. El término Resultado se utiliza para referirse a los resultados previstos, así como a los resultados reales. Véase también Objetivo.

Desempeño - Una medida de lo que se logra o entrega por un Sistema, persona, equipo, Proceso o Servicio de TI.

Gestión del rendimiento - Proceso responsable de las actividades diarias de gestión de la capacidad. Éstas incluyen la supervisión, la detección de umbrales, el análisis y el ajuste del rendimiento, y la aplicación de cambios relacionados con el rendimiento y la capacidad. Plan Una propuesta detallada que describe las Actividades y los Recursos necesarios para alcanzar un Objetivo. Por ejemplo, un Plan para implementar un nuevo Servicio o Proceso de TI. La ISO/IEC 20000 requiere un Plan para la gestión de cada Proceso de Gestión de Servicios de TI.

Tiempo de inactividad planificado - Tiempo acordado en el que un servicio de TI no estará disponible. El tiempo de inactividad planificado se utiliza a menudo para el mantenimiento, las actualizaciones y las pruebas. Véase también Tiempo de inactividad.

Política - Expectativas e intenciones de gestión formalmente documentadas. Las políticas se utilizan para orientar las decisiones y garantizar el desarrollo y la aplicación coherentes y adecuados de los procesos, las normas, las funciones, las actividades, la infraestructura informática, etc.

Revisión posterior a la implementación (PIR) - Una revisión que tiene lugar después de que se haya implementado un cambio o un proyecto. El PIR determina si el cambio o el proyecto ha tenido éxito e identifica las oportunidades de mejora.

Práctica - Una forma de trabajar, o una manera en la que se debe hacer el trabajo. Las prácticas pueden incluir actividades, procesos, funciones, normas y directrices. Véase también Buenas prácticas.

Problema - Causa de uno o más incidentes. La causa no suele conocerse en el momento en que se crea un Registro de Problema, y el Proceso de Gestión de Problemas es responsable de la investigación posterior.

Gestión de Problemas - El Proceso responsable de gestionar el Ciclo de Vida de todos los Problemas. Los objetivos principales de la Gestión de Problemas son evitar que se produzcan Incidentes y minimizar el Impacto de los Incidentes que no se pueden evitar.

Registro de Problema - Un registro que contiene los detalles de un problema. Cada registro de problema documenta el ciclo de vida de un solo problema.

Procedimiento - Documento que contiene los pasos que especifican cómo realizar una actividad. Los procedimientos se definen como parte de los procesos. Véase también Instrucción de Trabajo.

Proceso - Conjunto estructurado de actividades diseñadas para lograr un objetivo específico. Un proceso toma una o más entradas definidas y las convierte en salidas definidas. Un proceso puede incluir cualquiera de las funciones, responsabilidades, herramientas y controles de gestión necesarios para obtener los resultados de forma fiable. Un proceso puede definir políticas, normas, directrices, actividades e instrucciones de trabajo, si son necesarias.

Control de Procesos - Actividad de planificación y regulación de un Proceso, con el Objetivo de realizar el Proceso de manera Efectiva, Eficiente y consistente.

Gestor de procesos - Función responsable de la gestión operativa de un proceso. Las responsabilidades del Gestor de Procesos incluyen la planificación y coordinación de todas las actividades necesarias para llevar a cabo, supervisar e informar sobre el proceso. Puede haber varios Gestores de Procesos para un Proceso, por ejemplo, Gestores de Cambio regionales o Gestores de Continuidad de Servicios de TI para cada centro de datos. La función de Gestor de Procesos suele asignarse a la persona que desempeña la función de Propietario de Procesos, pero ambas funciones pueden estar separadas en las organizaciones más grandes.

Propietario del proceso - Función responsable de garantizar que un proceso sea adecuado para su finalidad. Las responsabilidades del Propietario del Proceso incluyen el patrocinio, el diseño, la gestión del cambio y la mejora continua del proceso y sus métricas. Esta función suele asignarse a la misma persona que desempeña la función de gestor de procesos, pero las dos funciones pueden estar separadas en organizaciones más grandes.

Calificación - Actividad que garantiza que la infraestructura de TI es adecuada y está correctamente configurada para soportar una aplicación o servicio de TI. Véase también Validación.

Garantía de calidad (QA) - Proceso responsable de asegurar que la calidad de un producto, servicio o proceso proporcionará el valor previsto.

RACI - Modelo utilizado para ayudar a definir las funciones y responsabilidades. RACI son las siglas en inglés de Responsable, Contable, Consultado e Informado. Véase también Parte interesada.

Registro - Documento que contiene los resultados u otros productos de un proceso o actividad. Los registros son una prueba del hecho de que una actividad tuvo lugar y pueden ser en papel o electrónicos. Por ejemplo, un informe de auditoría, un registro de incidentes o el acta de una reunión.

Recuperación: devolver un elemento de configuración o un servicio de TI a un estado de funcionamiento. La recuperación de un Servicio de TI a menudo incluye la recuperación de datos a un estado consistente conocido. Después de la Recuperación, pueden ser necesarios otros pasos antes de que el Servicio de TI pueda ser puesto a disposición de los Usuarios (Restauración).

Redundancia - Ver Tolerancia a fallos

Relación - Conexión o interacción entre dos personas o cosas. En la Gestión de Relaciones Empresariales es la interacción entre el Proveedor de Servicios de TI y la Empresa. En la Gestión de la Configuración es un enlace entre dos elementos de configuración que identifica una dependencia o conexión entre ellos. Por ejemplo, las aplicaciones pueden estar vinculadas a los servidores en los que se ejecutan, los servicios de TI tienen muchos vínculos con todos los CI que contribuyen a ellos.

Remediación - Recuperación a un estado conocido después de un Cambio o Liberación fallido.

Solicitud de cambio (RFC) - Una propuesta formal para realizar un cambio. Una RFC incluye detalles del cambio propuesto y puede registrarse en papel o electrónicamente. El término RFC se utiliza a menudo de forma errónea para referirse a un registro de cambio, o al cambio en sí.

Cumplimiento de solicitudes - El proceso responsable de gestionar el ciclo de vida de todas las solicitudes de servicio.

Requisito - Una declaración formal de lo que se necesita. Por ejemplo, un requisito de nivel de servicio, un requisito de proyecto o los resultados requeridos para un proceso.

Resiliencia: capacidad de un elemento de configuración o de un servicio informático de resistir un fallo o de recuperarse rápidamente después de un fallo. Por ejemplo, un cable blindado resistirá un fallo cuando se le someta a tensión. Véase también Tolerancia a los fallos.

Resolución - Acción tomada para reparar la Causa Raíz de un Incidente o Problema, o para implementar una Solución. En la norma ISO/IEC 20000, los procesos de resolución son el grupo de procesos que incluye la gestión de incidentes y problemas.

Capacidad de respuesta - Medición del tiempo que se tarda en responder a algo. Puede ser el tiempo de respuesta de una transacción, o la rapidez con la que un proveedor de servicios de TI responde a un incidente o a una solicitud de cambio, etc.

Restaurar - Tomar medidas para devolver un servicio de TI a los usuarios tras la reparación y recuperación de un incidente. Este es el objetivo principal de la gestión de incidentes.

Retorno a la normalidad - La fase de un Plan de Continuidad del Servicio de TI durante la cual se reanudan todas las operaciones normales. Por ejemplo, si un centro de datos alternativo ha estado en uso, entonces esta fase hará que el centro de datos primario vuelva a funcionar y restablecerá la capacidad de invocar los Planes de Continuidad del Servicio de TI de nuevo.

Revisión - Evaluación de un cambio, problema, proceso, proyecto, etc. Las revisiones suelen llevarse a cabo en puntos predefinidos del ciclo de vida, y especialmente después del cierre. El objetivo de una revisión es garantizar que se han proporcionado todos los productos finales e identificar las oportunidades de mejora. Véase también Revisión posterior a la implementación.

Derechos - Derechos, o permisos, concedidos a un Usuario o Rol. Por ejemplo, el derecho a modificar datos o a autorizar un cambio.

Riesgo - Un posible evento que podría causar daños o pérdidas o afectar a la capacidad de alcanzar los objetivos. Un Riesgo se mide por la probabilidad de una Amenaza, la Vulnerabilidad del Activo a esa Amenaza y el Impacto que tendría si se produjera.

Evaluación de riesgos - Los pasos iniciales de la gestión de riesgos. Analizar el valor de los activos para la empresa, identificar las amenazas a esos activos y evaluar la vulnerabilidad de cada activo a esas amenazas. La evaluación de riesgos puede ser cuantitativa (basada en datos numéricos) o cualitativa.

Gestión de riesgos - Proceso responsable de identificar, evaluar y controlar los riesgos. Véase también Evaluación de riesgos.

Rol - Conjunto de responsabilidades, Actividades y autoridades otorgadas a una persona o equipo. Un rol se define en un proceso. Una persona o equipo puede tener varios roles, por ejemplo, los roles de Gestor de Configuración y Gestor de Cambios pueden ser desempeñados por una sola persona.

Causa raíz - La causa subyacente u original de un incidente o problema.

Análisis de la causa raíz (ACR) - Actividad que identifica la causa raíz de un incidente o problema. El ACR suele centrarse en los fallos de la infraestructura de TI. Véase también Análisis de Fallos del Servicio.

Alcance - El límite, o la extensión, a la que se aplica un Proceso, Procedimiento, Certificación, Contrato, etc. Por ejemplo, el alcance de la gestión de cambios puede incluir todos los servicios de TI en vivo y los

elementos de configuración relacionados, el alcance de un certificado ISO/IEC 20000 puede incluir todos los servicios de TI prestados desde un centro de datos determinado.

Servicio - Un medio de proporcionar valor a los clientes facilitando los resultados que los clientes quieren lograr sin la propiedad de los costos y riesgos específicos.

Criterios de Aceptación del Servicio (SAC) - Conjunto de criterios utilizados para garantizar que un Servicio de TI cumple con su funcionalidad y sus Requisitos de Calidad y que el Proveedor de Servicios de TI está listo para Operar el nuevo Servicio de TI cuando se ha desplegado. Véase también Aceptación.

Activo de servicio - Cualquier capacidad o recurso de un proveedor de servicios. Véase también Activo.

Gestión de Activos y Configuración del Servicio (SACM) - El proceso responsable de la gestión de la configuración y de los activos.

Catálogo de Servicios - Una base de datos o un documento estructurado con información sobre todos los Servicios de TI vivos, incluidos los disponibles para su despliegue. El Catálogo de Servicios es la única parte de la Cartera de Servicios que se publica a los Clientes y se utiliza para apoyar la venta y entrega de Servicios de TI. El Catálogo de Servicios incluye información sobre los entregables, precios, puntos de contacto, pedidos y procesos de solicitud. Véase también Cartera de Contratos.

Contrato de servicios - Contrato para prestar uno o más servicios de TI. El término Contrato de Servicios también se utiliza para referirse a cualquier Acuerdo para prestar Servicios de TI, ya sea un Contrato legal o un SLA. Véase también Cartera de Contratos.

Cultura de Servicio - Una cultura orientada al cliente. Los principales objetivos de una cultura de servicio son la satisfacción del cliente y ayudar a los clientes a alcanzar sus objetivos empresariales.

Diseño del Servicio - Una etapa del Ciclo de Vida de un Servicio de TI. El Diseño del Servicio incluye una serie de Procesos y Funciones y es el título de una de las principales publicaciones de ITIL. Ver también Diseño.

Paquete de Diseño del Servicio - Documento(s) que define(n) todos los aspectos de un Servicio de TI y sus Requisitos a través de cada etapa de su Ciclo de Vida. Se produce un paquete de diseño del servicio para cada nuevo servicio de TI, cambio importante o retirada del servicio de TI.

Service Desk - El punto de contacto único entre el proveedor de servicios y los usuarios. Un Service Desk típico gestiona los incidentes y las solicitudes de servicio, y también se encarga de la comunicación con los usuarios.

Plan de Mejora del Servicio (SIP) - Un plan formal para implementar mejoras en un proceso o servicio de TI.

Sistema de Gestión del Conocimiento del Servicio (SKMS) - Conjunto de herramientas y bases de datos que se utilizan para gestionar el conocimiento y la información. El SKMS incluye el Sistema de Gestión de la Configuración, así como otras herramientas y bases de datos. El SKMS almacena, gestiona, actualiza y presenta toda la información que un proveedor de servicios de TI necesita para gestionar el ciclo de vida completo de los servicios de TI.

Nivel de servicio - Medición y comunicación de los logros respecto a uno o más objetivos de nivel de servicio. El término "nivel de servicio" se utiliza a veces de manera informal para referirse al objetivo de nivel de servicio.

Acuerdo de nivel de servicio (SLA) - Acuerdo entre un proveedor de servicios de TI y un cliente. El SLA describe el servicio de TI, documenta los objetivos de nivel de servicio y especifica las responsabilidades del proveedor de servicios de TI y del cliente. Un único SLA puede cubrir varios Servicios de TI o varios clientes. Véase también Acuerdo de Nivel Operativo.

Gestión del Nivel de Servicio (SLM) - El proceso responsable de negociar los Acuerdos de Nivel de Servicio y de garantizar su cumplimiento. El SLM es responsable de garantizar que todos los procesos de gestión de servicios de TI, los acuerdos de nivel operativo y los contratos de apoyo sean adecuados para los objetivos de nivel de servicio acordados. SLM supervisa e informa sobre los niveles de servicio y lleva a cabo revisiones periódicas de los clientes.

Paquete de Nivel de Servicio (SLP) - Un nivel definido de Utilidad y Garantía para un Paquete de Servicio particular. Cada SLP está diseñado para satisfacer las necesidades de un patrón de actividad comercial concreto.

Requisito de nivel de servicio (SLR) - Requisito del cliente para un aspecto de un servicio de TI. Los SLR se basan en los objetivos empresariales y se utilizan para negociar los objetivos de nivel de servicio acordados.

Objetivo de Nivel de Servicio - Un compromiso que se documenta en un Acuerdo de Nivel de Servicio. Los objetivos de nivel de servicio se basan en los requisitos de nivel de servicio y son necesarios para garantizar que el diseño del servicio de TI es adecuado para el propósito. Los objetivos de nivel de servicio deben ser SMART y normalmente se basan en KPIs.

Gestión de servicios: conjunto de capacidades organizativas especializadas para proporcionar valor a los clientes en forma de servicios.

Ciclo de vida de la gestión de servicios - Un enfoque de la gestión de servicios de TI que hace hincapié en la importancia de la coordinación y el control de las distintas funciones, procesos y sistemas necesarios para gestionar el ciclo de vida completo de los servicios de TI. El enfoque del Ciclo de Vida de la Gestión de Servicios considera la Estrategia, el Diseño, la Transición, la Operación y la Mejora Continua de los Servicios de TI.

Gestor de Servicios - Un gestor que es responsable de la gestión del ciclo de vida completo de uno o más servicios de TI. El término Gestor de Servicios también se utiliza para referirse a cualquier gestor dentro del Proveedor de Servicios de TI. Lo más habitual es que se refiera a un gestor de relaciones comerciales, un gestor de procesos, un gestor de cuentas o un directivo con responsabilidad sobre los servicios de TI en general.

Operación del Servicio - Una etapa del Ciclo de Vida de un Servicio de TI. La Operación del Servicio incluye una serie de Procesos y Funciones y es el título de una de las principales publicaciones de ITIL. Ver también Operación.

Propietario de Servicio - Un rol que es responsable de la entrega de un Servicio de TI específico.

Paquete de Servicios - Una descripción detallada de un Servicio de TI que está disponible para ser entregado a los Clientes. Un paquete de servicios incluye un paquete de nivel de servicio y uno o más servicios básicos y servicios de apoyo.

Service Pipeline - Una base de datos o un documento estructurado que enumera todos los servicios de TI que están en consideración o en desarrollo pero que aún no están disponibles para los clientes. El Service Pipeline proporciona una visión empresarial de los posibles servicios de TI futuros y forma parte de la cartera de servicios que normalmente no se publica a los clientes.

Cartera de Servicios - El conjunto completo de Servicios que son gestionados por un Proveedor de Servicios. La cartera de servicios se utiliza para gestionar todo el ciclo de vida de todos los servicios e incluye tres categorías: Cartera de Servicios (propuestos o en Desarrollo); Catálogo de Servicios (Activos o disponibles para su Despliegue); y Servicios Retirados. Véase también Gestión de la Cartera de Servicios, Cartera de Contratos.

Gestión de la Cartera de Servicios (SPM) - Proceso responsable de la gestión de la Cartera de Servicios. La Gestión de la Cartera de Servicios considera los servicios en términos del valor de negocio que proporcionan.

Informes de servicio - El proceso responsable de elaborar y entregar informes sobre los logros y las tendencias con respecto a los niveles de servicio. Los informes de servicio deben acordar el formato, el contenido y la frecuencia de los informes con los clientes.

Estrategia del Servicio - El título de una de las principales publicaciones de ITIL. La Estrategia del Servicio establece una estrategia general para los Servicios de TI y para la Gestión del Servicio de TI.

Transición del Servicio - Una etapa del Ciclo de Vida de un Servicio de TI. La Transición del Servicio incluye una serie de Procesos y Funciones y es el título de una de las principales publicaciones de ITIL. Ver también Transición.

Utilidad del Servicio - La funcionalidad de un servicio de TI desde la perspectiva del cliente. El valor de negocio de un servicio de TI se crea mediante la combinación de la utilidad del servicio (lo que hace el servicio) y la garantía del servicio (lo bien que lo hace). Véase también Utilidad.

Garantía de servicio - Garantía de que un servicio de TI cumplirá los requisitos acordados. Puede ser un acuerdo formal, como un acuerdo de nivel de servicio o un contrato, o puede ser un mensaje de marketing o una imagen de marca. El valor de negocio de un servicio de TI se crea mediante la

combinación de la utilidad del servicio (lo que hace el servicio) y la garantía del servicio (lo bien que lo hace). Véase también Garantía.

Especificación - Una definición formal de los requisitos. Una especificación puede utilizarse para definir requisitos técnicos u operativos y puede ser interna o externa. Muchas normas públicas constan de un código de buenas prácticas y una especificación. La especificación define la norma con la que se puede auditar a una organización.

Parte interesada - Todas las personas que tienen un interés en una Organización, Proyecto, Servicio de TI, etc. Las partes interesadas pueden estar interesadas en las actividades, los objetivos, los recursos o los resultados. Las partes interesadas pueden ser clientes, socios, empleados, accionistas, propietarios, etc. Véase también RACI.

Norma - Requisito obligatorio. Algunos ejemplos son la ISO/IEC 20000 (una norma internacional), una norma de seguridad interna para la configuración de Unix o una norma gubernamental sobre cómo deben mantenerse los registros financieros. El término norma también se utiliza para referirse a un código de prácticas o a una especificación publicada por una organización de normalización, como ISO o BSI. Véase también Directrices.

Cambio estándar - Un cambio preaprobado de bajo riesgo, relativamente común y que sigue un procedimiento o instrucción de trabajo. Por ejemplo, el restablecimiento de una contraseña o el suministro de un equipo estándar a un nuevo empleado. Los RFC no son necesarios para implementar un Cambio Estándar, y se registran y rastrean utilizando un mecanismo diferente, como una Solicitud de Servicio. Véase también Modelo de Cambio.

Estratégico - El más alto de los tres niveles de planificación y ejecución (estratégico, táctico y operativo). Las actividades estratégicas incluyen el establecimiento de objetivos y la planificación a largo plazo para lograr la visión general.

Estrategia - Un Plan Estratégico diseñado para alcanzar los Objetivos definidos.

Gestión de proveedores - Proceso responsable de garantizar que todos los contratos con los proveedores satisfagan las necesidades de la empresa y que todos los proveedores cumplan sus compromisos contractuales.

Grupo de Apoyo - Un grupo de personas con conocimientos técnicos. Los grupos de apoyo proporcionan el soporte técnico necesario para todos los procesos de gestión de servicios de TI. Véase también Gestión Técnica.

Servicio de apoyo - Un servicio que permite o mejora un servicio principal. Por ejemplo, un Servicio de Directorio o un Servicio de Copia de Seguridad. Véase también Paquete de servicios.

Sistema - Una serie de cosas relacionadas que funcionan juntas para lograr un Objetivo general. Por ejemplo:

- Un sistema informático que incluye hardware, software y aplicaciones
- Un Sistema de gestión, que incluye múltiples Procesos que se planifican y gestionan conjuntamente. Por ejemplo, un Sistema de Gestión de la Calidad
- Un sistema de gestión de bases de datos o sistema operativo que incluye muchos módulos de software que están diseñados para realizar un conjunto de funciones relacionadas.

Táctico - El medio de los tres niveles de planificación y ejecución (estratégico, táctico y operativo). Las actividades tácticas incluyen los planes a medio plazo necesarios para alcanzar objetivos específicos, normalmente durante un periodo de semanas a meses.

Gestión Técnica - Función responsable de proporcionar competencias técnicas en apoyo de los Servicios de TI y de la gestión de la Infraestructura de TI. La gestión técnica define las funciones de los grupos de apoyo, así como las herramientas, los procesos y los procedimientos necesarios.

Soporte técnico - Véase Gestión técnica.

Prueba - Actividad que verifica que un elemento de configuración, servicio de TI, proceso, etc., cumple con su especificación o con los requisitos acordados. Véase también Validación y Prueba del Servicio, Aceptación.

Entorno de prueba - Un entorno controlado utilizado para probar elementos de configuración, construcciones, servicios de TI, procesos, etc.

Costo total de propiedad (TCO): metodología utilizada para ayudar a tomar decisiones de inversión. El CTP evalúa el costo total del ciclo de vida de un elemento de configuración, no sólo el costo inicial o el precio de compra. Véase también Costo Total de Utilización.

Costo total de utilización (TCU) - Metodología utilizada para ayudar a tomar decisiones de inversión y contratación de servicios. El TCU evalúa el costo total del ciclo de vida para el cliente de la utilización de un servicio de TI. Véase también Costo Total de Propiedad.

Transición - Un cambio de estado, que corresponde a un movimiento de un servicio de TI u otro elemento de configuración de un estado del ciclo de vida al siguiente.

Planificación y apoyo a la transición - Proceso responsable de la planificación de todos los procesos de transición del servicio y de la coordinación de los recursos que requieren. Estos Procesos de Transición del Servicio son la Gestión de Cambios, la Gestión de Activos y Configuraciones del Servicio, la Gestión de Lanzamientos y Despliegues, la Validación y Pruebas del Servicio, la Evaluación y la Gestión del Conocimiento.

Contrato de apoyo (UC) - Un contrato entre un proveedor de servicios de TI y un tercero. El tercero proporciona bienes o servicios que apoyan la prestación de un servicio de TI a un cliente. El contrato de apoyo define los objetivos y las responsabilidades que se requieren para cumplir los objetivos de nivel de servicio acordados en un SLA.

Urgencia - Una medida de cuánto tiempo pasará hasta que un incidente, problema o cambio tenga un impacto significativo en el negocio. Por ejemplo, un incidente de alto impacto puede tener una urgencia baja, si el impacto no afectará al negocio hasta el final del año financiero. El impacto y la urgencia se utilizan para asignar la prioridad.

Usabilidad - La facilidad con la que se puede utilizar una aplicación, un producto o un servicio informático. Los requisitos de usabilidad suelen incluirse en una Declaración de Requisitos.

Caso de Uso - Una técnica utilizada para definir la funcionalidad y los objetivos requeridos, y para diseñar las pruebas. Los Casos de Uso definen escenarios realistas que describen las interacciones entre los Usuarios y un Servicio de TI u otro Sistema. Usuario Una persona que utiliza el Servicio de TI en el día

a día. Los usuarios son distintos de los clientes, ya que algunos clientes no utilizan el servicio de TI directamente.

Perfil de Usuario (UP) - Un patrón de demanda de Servicios de TI por parte del Usuario. Cada perfil de usuario incluye uno o más patrones de actividad empresarial.

Utilidad - Funcionalidad que ofrece un producto o servicio para satisfacer una necesidad concreta. La utilidad suele resumirse en "lo que hace". Véase también Utilidad del servicio.

Validación - Actividad que garantiza que un Servicio de TI, Proceso, Plan u otro Entregable nuevo o modificado satisface las necesidades del Negocio. La validación garantiza que se cumplan los requisitos del negocio aunque éstos hayan cambiado desde el diseño original. Véase también Verificación, Aceptación, Calificación, Validación y Prueba del Servicio.

Relación calidad-precio - Una medida informal de la rentabilidad. La rentabilidad suele basarse en una comparación con el costo de las alternativas.

Desviación - La diferencia entre un valor planificado y el valor real medido. Se utiliza habitualmente en la gestión financiera, la gestión de la capacidad y la gestión del nivel de servicio, pero puede aplicarse a cualquier ámbito en el que se apliquen planes.

Verificación - Actividad que garantiza que un Servicio de TI, Proceso, Plan u otro Entregable, nuevo o modificado, es completo, exacto, fiable y coincide con su especificación de diseño. Véase también Validación, Aceptación, Validación y Prueba del Servicio.

Verificación y Auditoría - Las actividades responsables de asegurar que la información en la CMDB es precisa y que todos los elementos de configuración han sido identificados y registrados en la CMDB. La verificación incluye comprobaciones rutinarias que forman parte de otros procesos. Por ejemplo, verificar el número de serie de un PC de escritorio cuando un usuario registra un incidente. La auditoría es una comprobación periódica y formal.

Versión - Una versión se utiliza para identificar una línea de base específica de un elemento de configuración. Las versiones suelen utilizar una convención de nomenclatura que permite identificar la secuencia o la fecha de cada línea de base. Por ejemplo, la Versión 3 de la Aplicación de Nómina contiene la funcionalidad actualizada de la Versión 2.

Visión - Una descripción de lo que la Organización pretende ser en el futuro. La visión es creada por la alta dirección y se utiliza para ayudar a influir en la cultura y la planificación estratégica.

Garantía - Promesa o garantía de que un producto o servicio cumplirá los requisitos acordados. Véase también Validación y pruebas del servicio, Garantía del servicio.

Instrucción de trabajo - Documento que contiene instrucciones detalladas que especifican exactamente los pasos a seguir para llevar a cabo una actividad. Una instrucción de trabajo contiene muchos más detalles que un procedimiento y sólo se crea si se necesitan instrucciones muy detalladas.

Solución - Reducir o eliminar el impacto de un incidente o problema para el que aún no se dispone de una resolución completa. Por ejemplo, reiniciando un elemento de configuración que ha fallado. Las soluciones para los problemas se documentan en los registros de errores conocidos. Las soluciones para los incidentes que no tienen registros de problemas asociados se documentan en el registro de incidentes.

Carga de Trabajo - Los Recursos requeridos para entregar una parte identificable de un Servicio de TI. Las cargas de trabajo pueden clasificarse por usuarios, grupos de usuarios o funciones dentro del servicio de TI. Se utiliza para ayudar a analizar y gestionar la capacidad, el rendimiento y la utilización de los elementos de configuración y los servicios de TI. El término Carga de Trabajo se utiliza a veces como sinónimo de Rendimiento.

2021-09-30/001

Idioma predominante:

En caso de discrepancia entre la versión original en inglés de este informe y la traducción al español, prevalece la versión en inglés.

Prevailing Language:

In the event of any discrepancy between the English original version of this report and the Spanish language translation, the English version prevails.