Glosario de términos de tecnologías de la información

1. Objetivo

Definir la terminología utilizada en la documentación de la Dirección de Servicios de Información y Tecnología (políticas, lineamientos, procesos, procedimientos, etc.), con el fin de utilizar un lenguaje unificado.

2. Términos y definiciones

Acceso confidencial: restricción sobre información que podría dañar o ser perjudicial a la seguridad de la Universidad si estuviera públicamente disponible.

Acceso restringido: restricción sobre información que podría producir efectos indeseados, si estuviera públicamente disponible.

Activo: (también tratado como Activo(s) de información) según (ISO/IEC 13335- 1:20041: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos de la Universidad. Se pueden clasificar de la siguiente manera:

Activo de información: los activos de información son los recursos que utiliza un sistema de Gestión de seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección. Los activos se encuentran asociados, de forma directa o indirectamente, con las demás entidades.

Administrador del sistema: es la persona que tiene la responsabilidad de implementar, configurar, mantener, monitorear, documentar y asegurar el correcto funcionamiento del sistema de información que se encuentre a su cargo.
Aprovisionador: sistema de información que permite gestionar las identidades de una organización. Mantiene organizada y unificada la información de los diferentes sistemas de la universidad, por ejemplo, cuentas de correo y acceso a otras plataformas tecnológicas.

Aceptación de riesgo: decisión de asumir un riesgo.

Acceso: nivel y alcance de la funcionalidad de un servicio o información que un usuario está autorizado a utilizar.

Acuerdo de nivel de servicio (SLA): Acuerdo documentado entre un proveedor de servicios y un cliente, en el que se especifican tanto los servicios requeridos como el nivel de servicio esperado.

Acuerdo a nivel de operación (OLA): acuerdo interno que cubre la prestación de servicios que da soporte a la unidad de Tecnología para la prestación y entrega de servicios.

Adaptabilidad: define que todos los eventos y bajo qué criterios un sistema debe poder ser monitoreado y revisado para su control posterior.

Amenaza: suceso de ocurrencia probable que puede desencadenar un incidente en la Universidad, produciendo daños o pérdidas materiales o inmateriales en los activos de información.

Ambiente de desarrollo: Ambiente que se utiliza para crear o modificar servicios de TI o aplicaciones.

Análisis de riesgos de seguridad: uso sistemático de la información para identificar fuentes y para estimar el riesgo (Guía ISO/IEC 73:2002). En tecnología se suele realizar un análisis de riesgos específico en cada uno de los tres procesos (incidentes, continuidad y seguridad), pero con objetivos.

Análisis Forense: es un conjunto de técnicas y herramientas de investigación basadas en tecnología, apoyadas en procesos documentados, para revisar en detalle el (los) incidentes de seguridad de la información designados.

Alta disponibilidad: es un diseño para alcanzar los niveles acordados de disponibilidad y para hacer uso de técnicas como la tolerancia a fallos, resistencia y recuperación rápida para reducir el número de incidentes y el Impacto de estos.

Aplicación: es un programa informático diseñado como herramienta para realizar funciones específicas para todos usuarios de la Universidad.

Áreas críticas de información: son aquellas áreas de la Universidad de los Andes que cuentan con un conjunto de activos de información. Por ejemplo, centros de cableados o centros de datos.

Arquitectura digital de referencia: es una guía que define cómo se estructuran, integran, restringen y coordinan las soluciones de TI de la Universidad de los Andes en los dominios de información, aplicaciones e infraestructura, y en los aspectos de seguridad, integración, procesos y costos.

Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Backup: respaldo o copia de seguridad.

Bases de datos: es un conjunto de información almacenada en recursos electrónicos.

Base de datos de conocimiento (KDB): es una base de datos lógica que contiene los datos e información requeridos por el Sistema de Gestión del Conocimiento del Servicio.

Base de datos de elementos de configuración (CMDB): es un repositorio que contiene todos los elementos de configuración, junto con sus datos, trazabilidad, relaciones y correspondencias.

Base de datos de errores conocidos (KEDB): es la base de datos que contiene todos los registros de errores conocidos, que proviene de información sobre solicitudes, incidentes y problemas.

Bimodal: es la práctica de administrar dos modos de trabajo separados pero coherentes: uno centrado en la operación; el otro en transformación o innovación. El modo 1 está orientado en áreas operativas o técnicas. Se enfoca en explotar y usar los recursos que ya se tienen y se conocen, sin dejar de lado su evolución de acuerdo al entorno. El modo 2 está orientado a la transformación y mejora continua para entregar a los usuarios servicios basados en experiencias, resolver y confrontar nuevos problemas. Ambos modos son esenciales para crear valor e impulsar un cambio organizacional significativo, y ninguno es estático. Ambos modos juegan un papel esencial en la transformación digital.

Bitácoras de respaldos y recuperaciones: son formatos digitales o físicos en los que se registra el resultado de las operaciones de respaldos y recuperaciones, permitiendo validar la efectividad y eficacia de los procesos de respaldo y recuperación.

Bus: ruta o canal de comunicación entre dispositivos de tecnologías de la información.

Cableado estructurado: es el conjunto de todos los componentes que se utilizan para la construcción de red, sistema de cables, conectores, canalizaciones y dispositivos que permiten establecer una infraestructura de telecomunicaciones.

Cambio estándar: es un cambio de un componente de infraestructura o servicio que la Gestión de Cambios debe registrar, pero que presenta un bajo riesgo y tiene autorización previa.

Cambio de emergencia: es un cambio que se realiza para reparar lo antes posible un fallo en un servicio de tecnología que tiene un gran impacto negativo sobre la Universidad.

- ✓ El sistema a ser cambiado no es crítico para el negocio.
- ✓ No se afecta el servicio de manera perceptible a los usuarios.
- ✓ No afecta significativamente la configuración o funcionalidad del sistema.

Cambio normal: son aquellos cambios que:

- ✓ Puede impactar en un grado alto la operación del servicio.
- ✓ Modifica la calidad del servicio.

- ✓ Modifica la configuración del sistema.
- ✓ Afecta la disponibilidad o desempeño del sistema a ser cambiado.
- ✓ Puede requerir el esfuerzo de equipos de trabajo, asignación de presupuestos.
- ✓ Requiere aprobación del CAB.

Campus agreement: software gestionado mediante acuerdos centrales. Por ejemplo, MICROSOFT, ADOBE, ENDNOTE, RESPONDUS, SPSS, STATA, SAS EAS, SAS DATA M, MATHEMATICA, MATLAB, LABVIEW, TERRSET, MATHCAD, CRYSTALL BALL, DROPBOX, MARKETING CLOUD, R25 LIVE, ANTIVIRUS, CLOUD – AZURE

Capacidad: es una aptitud, habilidad, competencia o recurso para poder implementar lo planteado en la intención. Una capacidad no es una intención sino una acción concreta, debe ser neutra en cuanto a los logros y a la manera en que se hace.

Catálogo de Servicios Tecnológicos: es un inventario o documento estructurado con información sobre todos los servicios de tecnología disponibles para Uniandes.

Catalizadores: son factores que, individual y colectivamente, influyen en algo que va a funcionar, en este caso, la gobernanza y la gestión a través de las tecnologías de la información.

Chatbot: plataforma de mensajería, red social o solución de chat para sus conversaciones.

Centro de cableado: es un sistema colectivo compuesto de cables, canalizaciones, etiquetas, espacios, conectores y otros dispositivos de red instalados para establecer una infraestructura de telecomunicaciones en un punto de operación. Es el punto central de una topología de red y sirve como el punto de unión central para el cableado y el equipo de cableado que se usa para conectar dispositivos en una red de área local (LAN).

Centro de costos: Unidad del negocio o proyecto al que se asignan los costos.

Centro de telecomunicaciones: es la ubicación física donde se concentran los recursos necesarios de computación de la Universidad o del proveedor de servicios.

Cintas magnéticas: también llamado volumen, es un medio magnético de almacenamiento secundario en el cual se coloca la información.

Ciclos de disrupción: transformaciones iterativas que cambian las expectativas y comportamientos fundamentales en una cultura, mercado, industria o proceso.

CIO (Chief Information Officer): director de información, supervisa a las personas, los procesos y las tecnologías dentro de la organización de TI de una empresa para garantizar que entreguen resultados que respalden los objetivos de la empresa.

Cifrado: proceso para tomar un mensaje no cifrado (texto sin formato), aplicarle una función matemática (algoritmo de cifrado con una clave) y producir un mensaje cifrado (texto cifrado).

Clasificación de incidentes y requerimientos: establece la categoría y prioridad de un incidente o requerimiento de tecnología.

Cliente-servidor: es un grupo de computadoras conectadas por medio de una red de comunicación, en la que el cliente es el dispositivo que solicitante un servicio al servidor, el cual es el proveedor de este. Sin embargo, puede trabajar en ambas vías.

Clustering: la capacidad de definir recursos en uno o más sistemas interconectados como disponibles de forma transparente para los usuarios y las aplicaciones integradas en una red.

Controles internos: políticas, procedimientos, prácticas y estructuras institucionales diseñadas para proporcionar un seguimiento y control sobre el logro de los objetivos, la mitigación de riesgos y la prevención y corrección de errores.

Control de cambios (proyectos): pertenece a un cambio solicitado por el Dueño funcional y que impacta el tiempo y/o el presupuesto ya acordado en el proyecto.

Comité de Cambios: es una reunión de personas convocada con el objetivo de aclarar y evaluar los cambios propuestos.

Comité de Seguridad de la Información: el comité de Seguridad de la Información, es un órgano de Gobierno de TI con integrantes y responsabilidades claramente definidas asegurar el cumplimiento de la estrategia de seguridad de la información de la Universidad.
Comunicaciones Unificadas: integración de los diferentes medios de comunicación que posee Uniandes, como voz, mensajería de texto y video en sus diferentes variantes, tanto en tiempo real como diferido, y sumando a la vez una gran cantidad de servicios de tecnología.

Comunidad Uniandina: conjunto de personas que poseen alguna relación con la Universidad (estudiantes, profesores, egresados, directivos, empleados y demás vinculados), quienes tienen derecho a la utilización de los servicios de la Universidad de los Andes y por ende deben conocer y cumplir las políticas, normas, lineamientos, procedimientos, que sean impartidos para el buen uso de los recursos y conservación de la buena imagen de la Institución.

Confiabilidad de la Información: garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones, los proyectos y la implementación de los diferentes planes estratégicos desarrollados en la Universidad.

Confidencialidad: acceso a la información por parte únicamente de quienes estén autorizados, característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Consecuencia: resultado de un evento que afecta los objetivos (IRAM-ISO 73:2013)

Contraseña: es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quienes no se les permite el acceso.

Control: las políticas, los procedimientos, los mecanismos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

Cookie: un código permanente colocado en un archivo en el disco duro de una computadora por un sitio web que el usuario ha visitado, con el fin de identificar y registrar a ese usuario y se puede acceder a él para diversos fines de marketing y seguimiento del sitio.

Correo electrónico: servicio de red que permite a los usuarios enviar y recibir mensajes, así mismo adjuntar archivos digitales. (también denominados mensajes electrónicos o cartas digitales) mediante redes de comunicación electrónica.

Computo en la nube: modelo para habilitar el acceso de red bajo demanda a un grupo compartido de recursos informáticos configurables que se pueden proporcionar rápidamente con un mínimo esfuerzo de gestión o interacción por parte del proveedor.
Cumplimiento: capacidad para demostrar la adherencia a los requisitos regulatorios y normativas legales externas e internas que apliquen a la Universidad y a las personas que la conforman.

Cuenta de usuario: es un objeto del Directorio activo que almacena información de las personas, con el fin de generar y permitir la gestión de las credenciales que les permiten tener acceso al computador y demás recursos definidos.

Cuenta impersonal: es una cuenta que no está asociada al nombre de una persona, sino que se crea con el nombre de un evento, grupo, etc. El responsable de la cuenta solo puede ser un funcionario de la universidad. Se debe definir con un nombre relacionado a su función.

Cuenta institucional: identificación de usuario con la que se puede acceder a los diferentes servicios informáticos que ofrece la Universidad de los Andes.

Cuenta de correo electrónico: cuenta de correo designada para gestionar temas exclusivos de la Universidad de los Andes.

Cultura digital: la cultura digital es el conjunto de normas, valores, significados y prácticas que determinan y definen el actuar de las personas dentro de la institución, en relación con el uso e interacción con las Tecnologías de la Información.

Dato personal: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Ley 1581 de 2012.

Dato sensible: información que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos (Decreto 1377 de 2013), entre otros, la captura de imagen fija o en movimiento, huellas digitales, fotografías, iris, reconocimiento de voz, facial o de palma de mano, etc..

Declaración de aplicabilidad: documento que describe los objetivos de control y los controles pertinentes y aplicables para el mismo.

Demanda: entrada al sistema de valores del servicio que se basa en las oportunidades y las necesidades de las partes interesadas internas y externas.

Derechos: también llamados privilegios. Hacen referencia a la configuración real de un usuario e indican los servicios o grupos de servicios que está autorizado a usar. Los derechos más habituales son los de lectura, escritura, ejecución, edición y eliminación.

Derechos de autor: aquella protección que le otorga el estado al creador de las obras literarias, científicas y artísticas desde el momento de su creación y por un tiempo determinado. Los derechos de autor cubren las obras artísticas, científicas y literarias; software y bases de datos, entre otros.

Deuda técnica: Lista de tareas que se deben volver a realizar y se acumularon como resultado de elegir soluciones temporales en vez de soluciones del sistema que tomarían más tiempo.

Desaprovisionar: acción o resultado de desproveer, desposeer, despojar o quitar permisos o privilegios.

Disponibilidad: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Dirección IP: un número binario único utilizado para identificar dispositivos en una red TCP / IP.

Directorio activo: el directorio activo es la herramienta de Microsoft para la organización y gestión de los recursos de una red; almacena información de computadores, usuarios, grupos, impresoras, permisos y servidores, entre otros.
Directriz: norma o conjunto de normas e instrucciones que se establecen o se tienen en cuenta al proyectar una acción o un plan. Marca las condiciones en que se genera algo.

Dueño de proceso: funcionario que tiene la responsabilidad del diseño, desarrollo, ejecución y desempeño de un proceso de negocio.

Dueño de servicio: funcionario que tiene la responsabilidad de velar por la seguridad de los servicios a su cargo.

Elemento de configuración (CI): Hace referencia a datos, información, programa, equipo, persona o cualquier otro recurso de tecnología utilizado en la prestación de los servicios. En el ámbito de seguridad se denomina “activo”, mientras que en el proceso de gestión de la configuración y en el resto de los procesos se utiliza el término “elemento de configuración”. Así, activo y elemento de configuración son conceptos similares.

Enclosure de discos: Se define como un equipo electrónico que se vale de un conjunto de algoritmos y técnicas que le permiten organizar grupos de discos duros de una tecnología y características técnicas dadas, de forma tal que los servidores puedan visualizar la data que reside en ellos utilizando estructuras lógicas.

Entorno de Prueba: Es un entorno controlado empleado para probar Ítems de configuración, creaciones, servicios de tecnología, procesos etc.

Equipo de cómputo: Es una máquina electrónica que recibe y procesa datos, para convertirlos en información y está constituido por dos partes esenciales hardware y software.

Equipo de gestión de información: equipo que se encarga de coordinar y organizar los procesos de acompañamiento y seguimiento en las áreas pedagógicas y administrativas para el correcto manejo de la información.

Equipo del proyecto: Se compone de los recursos a tiempo completo y parcial asignados para trabajar en los entregables del proyecto.

Épica: Una descripción de alto nivel de lo que necesita el usuario final, con un valor de negocio.

Error conocido: es un problema que tiene una causa raíz documentada y una solución definitiva y/o temporal. Los errores conocidos son creados y gestionados a través de su ciclo de vida por la gestión de problemas.

Escalado: transferir al nivel requerido para dar solución a los casos de tecnología que no son solucionados por el nivel actual, este escalado puede ser de tipo:

- ✓ Funcional: se requiere el apoyo de un especialista de mayor nivel para resolver la incidencia.
- ✓ Jerárquico: se debe acudir a un responsable de mayor autoridad para tomar decisiones que se escapan de las atribuciones asignadas al primer nivel, como asignación de tiempo y recursos adicionales para la solución de dicho incidente.

Escenarios de pruebas: Se generan a partir de los requerimientos del proyecto.

Evaluación del riesgo: es el proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Evento de seguridad de la información: Suceso identificado en un activo o elemento de configuración, que indica una posible brecha en la política de seguridad de la información, fallo de las salvaguardas o una situación que podría ser relevante para la seguridad.

Evidencia Objetiva: información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.

Experiencia del cliente: suma de las interacciones funcionales y emocionales con un servicio y un proveedor de servicios percibidas por el consumidor del servicio.

DSIT: Dirección de servicios de información y tecnología responsable de la plataforma tecnológica; gestiona y administra las Tecnologías de la Información, en apoyo a la actividad académica, creación e investigación, y administrativa de la Universidad de los Andes.

Garantía: certeza de que un producto o servicio cumplirá con los requerimientos acordados. La garantía se puede resumir como "la forma en que se entrega el servicio" y puede utilizarse para determinar si un servicio es "adecuado para el uso". A menudo, la garantía hace referencia a niveles de servicio que se alinean con las necesidades de los consumidores del servicio; se puede basar en un acuerdo oficial, o puede ser un mensaje de mercadotecnia o una imagen de marca. Normalmente la garantía afecta a áreas como la disponibilidad del servicio, su capacidad, los niveles de seguridad y la continuidad. Se puede

afirmar que un servicio proporciona un nivel de confiabilidad, o garantía, aceptable cuando se cumplen todas las condiciones definidas y acordadas.

Gerencia de proyectos de TI: es la aplicación de las mejores prácticas para la administración del ciclo de vida de un proyecto, con el fin de cumplir sus objetivos y alcanzar los beneficios esperados.

Gestión de servicios de TI: es el conjunto de actividades que garantiza la prestación de servicios de TI alineados con las necesidades de la Universidad y enfocados en la entrega de valor, a través de la correcta integración de personas, procesos y tecnologías.

Gestión de riesgos: es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

Gobierno de TI: el Gobierno de TI de la Universidad de los Andes es el sistema que permite dirigir y controlar el uso de las TI y, por lo tanto, provee herramientas para la definición, el monitoreo y el control del Plan Estratégico de Tecnologías de la información (PETI), define los órganos de Gobierno encargados de la toma de decisiones y la rendición de cuentas de TI, y establece los mecanismos para garantizar el cumplimiento de la normatividad interna y externa.

Grupo de distribución: es un grupo de usuarios (cuentas) que se utiliza para envío masivo de información.
Grupo de seguridad: es un grupo de usuarios (cuentas) que se utiliza para dar accesos a plataformas o aplicar reglas de forma masiva

Hardware: es la parte o conjunto físico de cualquier sistema informático, conformado por componentes eléctricos, electrónicos, electromecánicos y mecánicos. Utilizado para referirse a componentes físicos de tecnología como; equipos de cómputo, redes, periféricos, cableado o cualquier otro elemento físico.

Historia de usuario: Es una representación de un requisito escrito en una o dos frases utilizando el lenguaje común del usuario.

Impacto en el negocio: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones de la Universidad y amenazar la seguridad de la información. También el impacto está relacionado con el número de usuarios o sistemas afectados. Los criterios para definir el impacto deben estar definidos en los SLA.

Impacto en el servicio: efecto producido debido al cambio a realizar en la Infraestructura o el servicio de tecnología prestado.

Incidente: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Incidente mayor o de alta criticidad: es un suceso que causa interrupción de un servicio critico de tecnología de alto impacto para los usuarios o los procesos de la Universidad.

Incidente de seguridad de la información: un evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen la probabilidad significativa de comprometer las operaciones de la Universidad de los Andes, y amenazar la seguridad de la información. Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una omisión o violación a los controles de Seguridad de la Información definidos por la Universidad.

Información: conjunto organizado de datos procesados que constituye un activo esencial para las actividades de la Universidad.

Informe de seguridad: informe centrado específicamente en la seguridad, explicando los hechos acontecidos en el período. También puede haber un informe específico que detalle lo ocurrido en un incidente severo de seguridad.

Infraestructura tecnológica: agrupa y organiza el conjunto de elementos tecnológicos (hardware y software) que soportan las operaciones de la Universidad de los Andes.

Ingeniería Social: se denomina así a los métodos utilizados para obtener información a través de la manipulación de los usuarios legítimos. Algunos de los métodos más comunes son la suplantación telefónica, recolección de información de medios y documentos desechados y phishing.

Iniciativa: necesidad en proceso de formalización ante la DSIT.

Integridad: propiedad que busca mantener los datos libres de modificaciones no autorizadas, es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Internet de las Cosas (IoT): interconexión vía Internet de dispositivos que no se concibieron tradicionalmente como activos de TI, pero que ahora incluyen conectividad de red y competencias informáticas integradas.

Inventario de activos: lista de todos aquellos recursos físicos, de información, software, documentos, servicios, personas, reputación de la organización que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Invitado: persona externa que visita la Universidad.

Intranet: red informática interna que expone información a través de tecnologías Web para compartir recursos, información y servicios tecnológicos dirigidos a los colaboradores de la Universidad de los Andes.

Iteración: conjunto de actividades para obtener mínimo con un hito de negocio y con una duración máxima de 2 meses.

KPI: indicador clave de desempeño, es una medida del nivel del rendimiento de un proceso.

Kanban: método que permite visualizar el trabajo, identificar posibles bloqueos y conflictos entre recursos, y gestionar el trabajo en curso.

Máquina Virtual: equipo de cómputo basado en hardware virtual el cual es suministrado por un equipo físico acompañado de un software diseñado para virtualización

Madurez: medida de la confiabilidad, eficiencia y eficacia de una organización, práctica o proceso.

Métrica: medida o cálculo que se monitorea o informa con fines de gestión y mejora.

Modelo: representación de un sistema, una práctica, un proceso, un servicio u otra entidad que se utiliza para entender y predecir su comportamiento y sus relaciones

Monitorización de la seguridad. sistemas informáticos que supervisan y miden los controles de seguridad, y registran los eventos de seguridad.

Nivel de riesgo: grado de exposición a un riesgo.

NOC: (Network Operations Centers) es el área encargada de monitorear, dar mantenimiento, y solucionar los problemas en las redes de telecomunicaciones y elementos de infraestructura.

Librerías de respaldo: es un hardware que consta por lo general de un carrusel para almacenamiento de cintas, un brazo mecánico autónomo que tiene como objetivo la manipulación de los volúmenes para alimentar las unidades de cintas y su retorno posterior en el carrusel. También se encarga del proceso de limpieza de las unidades de cintas utilizando un volumen especial destinado para esos fines.

Licencia: documento que establece términos y condiciones para la compra, uso, instalación, copia, arriendo, backup o transferencia de un software. (este documento puede estar en formato físico o digital).

Líder funcional: es el rol responsable de definir las funcionalidades que debe poseer la solución, de forma tal que estas satisfagan los requerimientos del cliente, es importante tomar en consideración que este define el que de la solución y no el cómo de la misma.

Líder de aplicación/sistema: Es el rol responsable de la gestión técnica de una aplicación o sistema de información.

Lineamiento: es una orientación de carácter general, corresponde a una disposición o directriz que debe ser implementada.

Localidad segura de almacenamiento de cintas: es un sitio externo designado por UNIANDES cuya función es la de centro de acopio de las cintas usadas en los respaldos de los servidores.

Matriz de permisos: es la relación de responsabilidades con recursos para asegurar que cada tarea o actividad esté asignada a un cargo o a un equipo de trabajo.

Niveles de permisos: son un conjunto de permisos que se pueden asignar a un grupo específico para un objeto protegible concreto.

Norma: regla de conducta dictada o promulgada por un poder legítimo.

Perfil: es una categoría de usuario, constituida por un conjunto de permisos, es decir es una serie de acciones que puede realizar en cada sección.

Objetivo de control: situación o aspecto que se quiere alcanzar en el ámbito de la seguridad. La seguridad se implanta definiendo los objetivos de control necesarios.

Obras de cableado: son aquellas obras tecnológicas destinadas a la instalación, adecuación o ampliación de cableado estructurado en todo el sistema UNIANDES.

Parte interesada: es un conjunto de personas que tienen interés particular en la Universidad, proyecto, servicio de tecnología, etc., pueden interesarse en las actividades, objetivos, recursos o entregables. Pueden incluir clientes, usuarios, asociaciones, empleados, propietarios, etc.

Perfil de usuario: es un entorno personalizado asociado a un servicio de tecnología que contiene la información básica del usuario.

Política: es una actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos.

Phishing: también llamado suplantación de identidad y consiste en el envío masivo de mensajes electrónicos que fingen ser notificaciones oficiales de empresas legítimas con el fin de obtener datos personales de usuarios.

Plan estratégico de tecnologías de la información (PETI): es un artefacto para expresar la Estrategia de la Gerencia de Servicios Tecnológicos, que hace parte integral de la estrategia general de la Universidad y es el resultado de un adecuado ejercicio de planeación estratégica de TI.

Plan de Continuidad de los Servicios de TI: plan que define los pasos necesarios para recuperar uno o más servicios de tecnología. El Plan además identificará los disparadores de la Invocación del plan, las personas que han de ser involucradas, las comunicaciones necesarias etc. El plan de continuidad de los Servicios de TI debería ser parte de un Plan de Continuidad del Negocio.

Plan de Continuidad del Negocio: plan que define los pasos que se requieren para el restablecimiento de los procesos críticos de la institución después de una interrupción. El plan también identifica los disparadores para la invocación, las personas involucradas, las comunicaciones, etc.

Plan de implementación del sistema de seguridad de la información: es un plan para el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la información de UNIANDES, con el objetivo de asegurar la integridad, disponibilidad y confidencialidad de los activos de información minimizando los riesgos de seguridad de la información.

Plan de Mejora de Servicio: es un plan formal para implementar mejoras a un Proceso o Servicio de tecnología.

Plan de rollback: es un plan que se establece dentro del proceso de la gestión de cambios para describir las actividades que permiten retornar a la última versión estable o inicial cuando la ejecución del cambio falla o no es exitoso.

Plataforma de Colaboración y Productividad: son plataformas digitales alojadas en la Web que facilitan la colaboración entre personas y equipos, la movilidad y la productividad, ofreciendo una serie de herramientas integradas tales como correo electrónico, almacenamiento en línea, chats, video-conferencia, creación y edición de contenido, entre otras; a las cuales se puede tener acceso desde múltiples dispositivos electrónicos conectados Internet.

Plataforma Tecnológica: sistema base de integración de infraestructura de TI, sistemas de información, bases de datos, plataformas de cómputo, servicios de tecnologías de la información, Sistemas de comunicaciones unificadas, sistemas telemáticos, redes de datos y herramientas informáticas definidas por UNIANDES para la prestación de servicios tecnológicos.

Política de retención de la información: es un parámetro que describe el período en el cual la data respaldada en un volumen se considera como válida. Es decir, luego de respaldar la información en cinta se establece que la misma durará un tiempo predefinido registrado en el sistema como válida. Al vencer dicho intervalo, el volumen se considera como expirado y la data podrá ser eliminada, permitiendo el reciclaje de los volúmenes.

Prioridad: es el resultado del cálculo de la interacción entre dos reglas (impacto y urgencia) que permiten definir el orden de resolución.

Probabilidad: frecuencia con la que puede ocurrir un suceso, o la relación entre el número de casos favorables y el número de casos totales.

Procedimiento: documento que permite conocer un método o manera de ejecutar algo. son los criterios establecidos sobre un proceso.

Proceso: es un conjunto de procedimientos o funciones que tienen uno o más objetivos.

Procesos misionales: son los procesos esenciales de una institución.

Procesos de apoyo: son todos aquellos procesos para la provisión de los recursos que son necesarios en los procesos estratégicos, misionales y de medición, análisis y mejora.

Propietario o Dueño de la aplicación: funcionario designado para indicar las limitaciones de uso, modificación o redistribución de la aplicación, además de su licencia y costo.

Propietario o Dueño de la información: funcionario que tiene la responsabilidad de garantizar que la información se clasifique adecuadamente, además de ser responsable de definir y revisar periódicamente las restricciones de acceso a la misma, tiene la potestad de tomar decisiones sobre la información.

Proveedor, contratista o tercero: persona externa que presta servicios a la Universidad a través de un contrato.

Proceso de negocio: es un grupo de actividades asumidas por la Universidad en la búsqueda de un objetivo común.

Propiedad intelectual: conjunto de derechos y prerrogativas sobre todas las creaciones del ingenio humano en cualquier campo del saber y respecto de los cuales el Estado y la legislación vigente ofrecen especial protección. La propiedad intelectual comprende: derecho de autor y derechos conexos, propiedad industrial y títulos de obtenciones vegetales.

Proyecto: esfuerzo temporal planeado para la construcción de una solución. Debe tener un alcance definido, un costo asociado, y debe generar mínimo un entregable funcional y técnico.

Prueba: es una actividad que verifica que un elemento de configuración, servicio de tecnología, proceso, etc. cumple con las especificaciones o requerimientos acordados.

Prueba de carga: Pruebas de concurrencia que buscan medir el desempeño de un sistema o componente de software, a una determinada carga de trabajo durante un tiempo, o validar la máxima carga soportada (estrés). Estas pruebas son importantes realizarlas sobre un ambiente de pruebas o pre-productivo.

Pruebas de integración: pruebas de caja gris que buscan validar que todos los componentes de un software funcionan correctamente juntos. Se enfocan principalmente en las interfaces entre componentes y validan que la comunicación entre estos sea correcta. Estas pruebas son incluidas en la fase de construcción y son planeadas y ejecutadas en conjunto por el equipo de desarrollo y de QA de los CedEx involucrados.

Pruebas de regresión: pruebas que buscan validar que no haya nuevos errores al ingreso de un nuevo cambio o evolución del software. Estas pruebas son ejecutadas por el equipo de desarrollo y de QA de los CedEx.

Pruebas de sistema de aceptación: prueba para garantizar que el sistema realiza correctamente todas las funcionalidades que se han detallado en las historias de usuario y las ejecutan los Gestores de valor.

Prueba unitaria: pruebas de caja blanca enfocadas en validar el correcto funcionamiento de segmentos o unidades de código que realizan cierta tarea. Estas pruebas son incluidas en la fase de construcción de la aplicación por parte del equipo de desarrollo.

Pruebas de seguridad: esta clase de pruebas buscan certificar que la aplicación cumple con los mínimos requeridos de seguridad, como son: confidencialidad, integridad, no repudio, autenticidad y responsabilidad. Estas pruebas se pueden incluir previo al despliegue a producción.

Solicitud de cambio: (RFC, Request For Change). es el medio para proponer un cambio en cualquier activo o elemento de configuración o en cualquier aspecto de un servicio de tecnología.

RAEEs: manejo integral de residuos de aparatos eléctricos y electrónicos generados en todas las sedes y lugares de operación de la Universidad de los Andes desde su identificación, separación en la fuente, recolección, transporte interno, almacenamiento, tratamiento y disposición final.

Recuperación: es el proceso mediante el cual se extrae información respaldada en una fecha pasada, en un medio de almacenamiento ya sea cinta magnética o unidad de discos.

Red LAN: sistema de comunicaciones capaz de facilitar el intercambio de datos informáticos entre los equipos de cómputo y los usuarios.

Red WAN: es un tipo de red que cubre distancias de entre unos 100 y unos 1.000 kilómetros, lo que le permite brindar conectividad.

Requerimiento del usuario: contacto del usuario para solicitar la provisión de una funcionalidad individual de un servicio de tecnología, asesoramiento, información, un cambio estándar o acceso a un Servicio de tecnología.

Respaldo de información: es una copia de la información que reside en algún dispositivo de almacenamiento digital, ya sea en forma de un disco duro de un servidor o una máquina virtual. Por lo general la copia se realiza con unidades de respaldos y recuperaciones. El medio más común de almacenamiento son las cintas magnéticas.

Respaldo diario: es aquella copia de seguridad que realiza la herramienta de respaldos y recuperaciones de forma automática y su frecuencia es diaria. Por lo general su modalidad es incremental.

Respaldo full: consiste en respaldar la totalidad de los datos almacenados en una ruta especifica. Es también un requisito indispensable para generar las copias de seguridad incrementales. Las copias de respaldo full implican una alta demanda en los recursos de almacenamiento requeridos para salvaguardar la información, así como un tiempo considerable de ejecución. Pueden causar inconvenientes de desempeño en la prestación de un servicio determinado, situación que depende de la cantidad de información a respaldar. Por tal razón, son procesos que se ejecutan en horarios de poca afluencia de usuarios.

Respaldo full sintético: consiste en una copia de seguridad integrada de una copia de seguridad completa (no sintetizada) anterior y tradicional, y copias de seguridad diferenciales subsiguientes o una copia de seguridad incremental acumulativa. Puede usar la copia de seguridad sintetizada para restaurar archivos y directorios de la misma manera en la que se realiza restauraciones desde una copia de seguridad tradicional.

Respaldo incremental: consiste en respaldar todos aquellos archivos que hayan sido modificados o creados a partir de la última copia de respaldo full. Las copias de respaldo incrementales implican una menor demanda en los recursos de almacenamiento requeridos para salvaguardar la información debido a que la cantidad de datos que se respaldan es mucho menor. Sin embargo, es requerida la existencia de una copia de respaldo full previo, a partir del cual se realizan los procesos de comparación para determinar cuáles archivos han sido modificados o creados y deben ser respaldados. El tiempo de ejecución de este tipo de copia es considerablemente menor en comparación con el full y normalmente no implican inconvenientes de desempeño en la prestación de un servicio determinado.

Respaldo mensual: es una copia de seguridad que se realiza una vez al mes, la modalidad es "Full" y la herramienta de respaldos y recuperaciones las ejecuta de forma automática.

Respaldo semanal: es un duplicado de seguridad que la herramienta de respaldos y recuperaciones ejecuta de forma programada, la frecuencia de estas copias es semanal. La modalidad debe ser "Full", debido a que sirve de punto de referencia para los respaldos incrementales diarios.

Respaldo por demanda: son copias en modalidad completa de uno o más servidores y las solicita un usuario o área. Una de las razones más comunes para este tipo de respaldos, es la futura eliminación de la información que reside en un servidor.

Restauración: acciones tomadas para restaurar el servicio de tecnología a los usuarios de UNIANDES tras reparar o solucionar un incidente.

Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. combinación de la probabilidad de un evento y sus consecuencias.

Rol: es una colección de permisos definida para todo un sistema, se puede asignar a usuarios específicos en contextos específicos.

Segregación de funciones: es el método para separar las responsabilidades de las diversas actividades que intervienen en la elaboración de los estados financieros, incluyendo la autorización y registro de transacciones, así como mantener la custodia de activos.

Seguridad informática: gestión de la implementación y mantenimiento de las herramientas y controles establecidos a nivel de hardware, software y organizacional para la seguridad de la información.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.
Servicios de TI: es un conjunto de actividades que buscan responder a las necesidades de un cliente por medio de un cambio de condición en los bienes informáticos, potenciando el valor de estos y reduciendo el riesgo inherente del sistema.

Servicios en la nube: (Cloud Computing), es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.

Servidor: es una aplicación en ejecución (software) que, formando parte de una red, provee servicios a los clientes y usuarios de UNIANDES.

Sistema Integral de Servicio: es el sistema de información sobre el cual se registran las solicitudes de servicio (tanto incidentes como requerimientos) y se gestionan hasta su cierre.

Sistema de gestión de la seguridad de la Información: conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Sistema de gestión del servicio de TI (SGSTI): es un sistema de gestión o modelo formalizado con el que se gestionan los servicios de las TI. La norma ISO/IEC 20000 define este sistema de gestión.

Sistema de gestión de la seguridad de la información (SGSI): parte del sistema de gestión global. Es un conjunto de políticas de administración de la información que propende por el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información.

Sistema de información: Conjunto de componentes y unidades de software interrelacionados que permiten el registro, proceso, almacenamiento, distribución y consulta de información, oportuna, relevante y eficaz para la toma de decisiones estratégicas de UNIANDES.

Sistema de respaldo y recuperación: Es un sistema que permite almacenar y recuperar información desde y hacia medios de almacenamiento secundarios. Genera además estadísticas y un inventario detallado de todas las operaciones que se realizan sobre la información y los medios de almacenamiento. Puede integrarse con dispositivos de almacenamiento tales como unidades de respaldo a disco y librerías de respaldo a cintas magnéticas.

Sistema de detección de intrusiones (IDS): inspecciona la actividad de seguridad de la red y del host para identificar patrones sospechosos que pueden indicar un ataque a la red o al sistema

Slot de cintas: es una ubicación numerada dentro del carrusel de cintas, en la cual se colocan los volúmenes para luego ser manipulados por el brazo mecánico de la librería.

SLR (service level requirement): requisito de nivel de servicio es un requisito del cliente para un aspecto de un servicio de TI. Los SLRs se basan en objetivos de negocio y se usan para negociar los acuerdos de nivel de servicio.

Snapshot: es una copia en disco de los apuntadores correspondientes a bloques de las LUN's. Se utiliza para reconstruir la información contenida en ellas en un período de tiempo específico.

Software: conjunto de aplicativos y programas que están instalados en cada uno de los equipos de cómputo para realizar determinadas tareas.

Software libre: es considerado software libre aquel que otorga a los usuarios las cuatro libertades: libertad 0, es la libertad de ejecutar el programa como se desee con cualquier propósito. Libertad 1, es la libertad de estudiar cómo funciona el programa, y cambiarlo para que haga lo que usted quiera. Libertad 2, es la libertad de redistribuir copias para ayudar a otros. Libertad 3 es la libertad de distribuir copias de sus versiones modificadas a terceros.

Solicitud de Cambios RFC (Request for Change): es una petición formal para cambiar uno o más elementos de configuración.

Suscripción: tipo de licenciamiento que se paga por consumo o por accesos.

Switch: elemento de configuración que permite la conexión de computadoras y periféricos a la red para que puedan comunicarse entre sí y con otras redes.

Tecnología de la información (TI): las TI abarcan el dominio completo de la información, que incluye al hardware, al software, a los periféricos y a las redes. Aplicación de computadores y equipos de telecomunicación que permiten almacenar, recuperar, transmitir y manipular datos, utilizado en el contexto de los negocios u organizaciones.

Tratamiento del riesgo: es el proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.

Contratos (UC): es un contrato entre un proveedor de servicios de TI y un tercero. El tercero proporciona bienes o servicios que soportan la entrega de un servicio de TI a clientes. El contrato de apoyo define objetivos y responsabilidades que son requeridas para alcanzar objetivos de nivel de servicio en uno o más SLA.

Unidades de respaldos y recuperaciones: dispositivos electrónicos que se encargan del manejo de las operaciones (escritura / lectura / preparación) de los volúmenes a bajo nivel.

UPS: elemento de configuración que sirve como fuente de suministro eléctrico y que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica.

Urgencia: se refiere a la rapidez requerida para resolver un incidente de un determinado impacto. Generalmente viene determinada por el tiempo disponible para la resolución del incidente sin afectar al servicio.

Usuario: persona vinculada a la Universidad de los Andes mediante una relación contractual, o ex contractual, al cual se le concede el acceso para el uso de la información, los servicios y las plataformas tecnológicas de la Universidad.

Valoración del riesgo: Es el proceso de análisis y evaluación del riesgo.

Virus: programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tardo tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

Visitante o invitado: persona externa que visita la Universidad de los Andes.

VPN: *Virtual Private Network* y que a su vez traduce red privada virtual, es una tecnología que permite generar conexiones seguras de forma remota cifrando la conexión entre los extremos bien sea entre una computadora y una red o entre dos redes diferentes a pesar que trasmiten datos por internet como si fueran la misma red.

Vulnerabilidad: debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

3. Roles

Clasificación	Nombre del rol	Definición
Roles en la comunidad Uniandina	Empleado	Persona que trabaja con un contrato laboral firmado con la Universidad de los Andes. Tanto los profesores como los administrativos están incluidos en esta categoría.
	Estudiante	Persona que cursa estudios de pregrado o posgrado en la Universidad de los Andes.
	Egresado	Persona que ha concluido sus estudios y obtenido un título de la Universidad de los Andes.
	Proveedores y terceros	Persona natural o jurídica externa que presta servicios a la Universidad a través de un contrato.
	Visitantes o Invitados	Persona externa que visita la universidad.
Órganos de Gobierno	Rector	Representante legal de la Universidad. Le corresponde dirigir académica, administrativa y financieramente a la Universidad, de conformidad con las políticas y decisiones del Consejo Superior y del Comité Directivo.
	Consejo académico	Órgano de gobierno de la Universidad compuesto por el Rector, quien lo preside, los Vicerrectores, los Decanos y los directores de unidades académicas que según reglamentación del Comité Directivo deben formar parte de él. Igualmente, lo conforman un profesor y un estudiante, nombrados por el Comité Directivo para un período de un año, prorrogable por una sola vez.
Comités	Comité de Seguridad de la Información	Comité de toma de decisiones institucionales en relación con la Seguridad de la información. Está conformado por un representante de la Dirección jurídica, un representante de Auditoría interna, un representante de Gestión humana, la Secretaría General, el Director de la DSIT y un representante del equipo de Seguridad de la información.
	Comité Operativo de Seguridad de la Información	Expertos en seguridad informática de los diferentes equipos de la DSIT que tienen a su cargo la administración de servicios informáticos o plataformas tecnológicas de la Universidad.
	Comité de Continuidad	Grupo de funcionarios representantes de las diferentes áreas de la Universidad a quienes han encargado la construcción del plan de continuidad de la Universidad de los Andes.
Vicerrectorías	Vicerrectoría Administrativa y Financiera	Unidad encargada de la gestión administrativa y financiera de la Universidad.

	Vicerrectoría de Desarrollo y Egresados	Unidad encargada del relacionamiento externo de la Universidad.
Direcciones y Jefaturas	Dirección de Admisiones y Registro	Unidad encargada de la gestión administrativa de la historia académica de los estudiantes y egresados de la Universidad.
	Dirección de Gestión Humana y Desarrollo Organizacional	Unidad encargada de la gestión y el desarrollo del talento humano en la Universidad.
	Dirección de Servicios de Información y Tecnología	Unidad encargada de la gestión de las Tecnologías de la información en la Universidad.
	Dirección Jurídica	Unidad encargada de asesorar jurídicamente a los órganos y autoridades administrativas de la Universidad.
	Gerencia del Campus	Unidad encargada de proveer los recursos físicos requeridos para la operación de la Universidad.
	Jefatura de Administración Documental	Unidad encargada de gestionar y regular el ciclo de vida documental de la información institucional.
	Jefatura de Seguridad y servicios básicos	Unidad encargada de la seguridad física y de la prestación de servicios básicos en el campus.
Cargos	Director de Unidad	Persona de cargo directivo con potestad de autorización dentro de su unidad en la Universidad.
	Jefe de área	Persona de cargo directivo, responsable de un equipo de trabajo con funciones específicas. Es el cargo siguiente a Director de Unidad.
Funciones	Mesa de Servicio	Grupo de atención de primer nivel y punto único de contacto para la atención a los usuarios de servicios de tecnología.
	Administrador de área Física	Funcionario encargado o responsable de la administración y los accesos a áreas de la Universidad que cuentan con acceso restringido (ej.: laboratorios).
	Dueño de proceso	Funcionario que tiene la responsabilidad del diseño, desarrollo, ejecución y desempeño de un proceso de negocio.
	Propietario de la información	Funcionario que tiene la responsabilidad de garantizar que la información se clasifique adecuadamente, además de ser responsable de definir y revisar periódicamente las

		restricciones de acceso a la misma, tiene la potestad de tomar decisiones sobre la información.
	Dueño de la aplicación/servicio	Persona responsable de coordinar la definición de las necesidades existentes en la organización y transformarlas en requerimientos. Este rol ejecuta como cliente final ante el equipo técnico, ya que es quien consolida la información proveniente de las necesidades de los usuarios solicitantes.
	Administrador de la aplicación/sistema	Persona que tiene la responsabilidad de implementar, configurar, mantener, monitorear, documentar y asegurar el correcto funcionamiento del sistema de información que se encuentre a su cargo.
	Responsable de desarrollo	Persona encargada del grupo especializado en elaborar sistemas de información para la Universidad, en el marco de un proyecto.
	Supervisor del contrato	Empleado que ha sido delegado por la Universidad para realizar las labores de control y verificación de los contratos suscritos con proveedores o contratistas.

4. Referencias

La construcción de este glosario se basa en definiciones tomadas de las siguientes fuentes:

- ✓ Operación del Servicio Basada en ITIL® V3 - Guía de Gestión - https://www.academia.edu/13256871/Gu%C3%ADa_de_gesti%C3%B3n_de_servicios_basada_en_Fundamentos_de_ITIL_v3.
- ✓ ISO 20000 - Calidad de los servicios TI ISO / IEC 20000. Normalizada y publicada por las organizaciones ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) el 14 de diciembre de 2005.
- ✓ Cobit 5 visión empresarial del Gobierno de TI, 10 de abril de 2012.
- ✓ Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) https://www.mintic.gov.co
- ✓ Gartner IT Glossary.
- ✓ ISACA Glossary of Terms.
- ✓ Definiciones de la norma ISO 38500.
- ✓ PMBOK sexta edición.
- ✓ Definiciones del marco de referencia de Arquitectura empresarial de Arquitectura TI Colombia.
- ✓ Sitio web https://www.gnu.org/.

5. Versión

Versión	Descripción	Actualizado por	Fecha
1.0	Creación del documento	Oscar Fonseca	05/03/2020
2.0	Actualización definiciones	Oscar Fonseca	07/07/2020

6. Aprobación

	Nombre	Cargo	Fecha
Elaboró	Oscar Fonseca	Ingeniero de gobierno TI	05/03/2020
Revisó	Eliana Benitez	Ingeniero de planeación	06/03/2020
Aprobó	Diana Garzón	Coordinador de Gobierno TI	06/03/2020