



RESOLUCIÓN No. 39 DE 2020
(Diciembre 17)

**POR LA CUAL SE ESTABLECE LA POLÍTICA INTEGRAL DE TECNOLOGÍAS
DE LA INFORMACIÓN**

El Rector de la Universidad Simón Bolívar en uso de sus atribuciones estatutarias y en atención a los siguientes

CONSIDERANDOS:

1. Que el Acuerdo de la Sala General No. 1 de 2020 define la normalización de la ley de tratamiento de la información con el fin de atender las políticas institucionales en materia de los principios rectores de responsabilidad y protección de datos, conforme a la Ley 1581 de 2012 y el Decreto 1377 de 2013.
2. Que el proceso de gestión de TI es transversal en el desarrollo de la organización y se orienta a la generación de valor a través de las TIC.
3. Que el Plan Estratégico de Desarrollo de la Universidad establece como uno de los objetivos de los lineamientos estratégicos de TI, generar e implementar soluciones de innovación tecnológicas, que permitan el mejoramiento y fortalecimiento continuo de la calidad de los servicios.
4. Que dentro de los diferentes cambios que han ocurrido en el ámbito de las TIC's, el Estado colombiano ha emitido leyes, decretos y normas para fomentar y fortalecer el buen uso de las TIC en todo el territorio nacional.
5. El artículo 2.2.9.1.2.1. del Decreto 1078 de 2015, también subrogado por el artículo 1 del Decreto 1008 de 2018, estableció que la Política de Gobierno Digital se desarrollará a través de componentes y habilitadores transversales y respecto de estos últimos indica que son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.
6. Que, las políticas institucionales deberán atender a la normatividad vigente en materia de protección de datos, propiedad intelectual, responsabilidad social y ambiental, así como las que estime necesarias para responder a las expectativas, necesidades y contextos locales, regionales y globales conforme al Artículo 2.5.3.2.3.1.3. Estructura administrativa y académica del decreto 1330 de 2019 del Ministerio de Educación Nacional.





Por lo anteriormente expuesto, el Rector de la Universidad Simón Bolívar,

RESUELVE:

Aprobar la Política Integral de Tecnologías de la Información como documento que se desarrolla dentro de las funciones sustantivas y administrativas de la Universidad y comprende los siguientes artículos:

artículo 1.	Información del responsable del proceso de gestión TI.....	2
artículo 2.	Objetivo.....	2
artículo 3.	Alcance y aplicabilidad	3
artículo 4.	Marco normativo	3
artículo 5.	Definiciones.	5
artículo 6.	Política integral de tecnologías de la información.....	10
artículo 7.	Principios activos de la política integral de TI.....	10
artículo 8.	Dominios.....	12
artículo 9.	Referencias, estándares, políticas y procesos relacionados	26
artículo 10.	Indicadores.	26
artículo 11.	Excepciones.	28
artículo 12.	Revisiones y actualizaciones.	28
artículo 13.	Sanciones.....	28
artículo 14.	Vigencia, derogatoria y socialización	28
artículo 15.	Cumplimiento.....	28

Artículo 1. Información del responsable del proceso de gestión TI.

1. Razón social: UNIVERSIDAD SIMÓN BOLÍVAR
2. Número de Identificación Tributaria: 890.104.633-9
3. Dirección – domicilio: Calle 58 #55-132, Barranquilla, Atlántico, y Calle 15 #142, Cúcuta, Norte de Santander
4. Teléfono: (57+5) 3444333 en Barranquilla y (57+7) 5827070 en Cúcuta
5. Departamento de Tecnologías de la información: Proceso Gestión de TI
6. Sitio Web: www.unisimon.edu.co

Artículo 2. Objetivo.

El objetivo de la política Integral de TI de la Universidad Simón Bolívar es establecer los lineamientos que permitan asegurar el aprovisionamiento, uso y soporte de la operación, procesos y capacidades de la arquitectura TI, servicios y Seguridad y privacidad con el fin de impulsar el aprovechamiento de los recursos tecnológicos que aseguren el cumplimiento de las actividades relacionadas a cada uno de los procesos institucionales de manera óptima y de calidad.





Artículo 3. Alcance y aplicabilidad.

La Política Integral de TI es aplicable a todos los niveles de la Universidad Simón Bolívar, pasando por gestores de TI, directivos, funcionarios, Profesores, contratistas, estudiantes, proveedores, colaboradores y visitantes, donde desarrollen, utilicen, recolecten, procesen, intercambien o consulten los activos de información habilitados de manera transversal por el Marco de Arquitectura Empresarial que enmarca en los dominios de estrategia de TI, gobierno TI, Información, sistemas de información, sistemas tecnológicos, uso y apropiación.

Contempla los lineamientos requeridos para normalizar el PETIC en la Universidad Simón Bolívar, definición de la Política de TI, principios, marco normativo, la definición de los indicadores para el monitoreo de cumplimiento de la política, hasta la definición de una estrategia para la adopción de la política para la Institución.

Artículo 4. Marco Normativo.

1. Constitución:

Constitución Política. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data; Artículo 20. Libertad de Información.

2. Leyes:

- a) Ley 80 de 1993: Mediante el cual se establecen las pautas de Contratación con el Estado Colombiano.
- b) Ley 527 de 1999. "Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"
- c) Ley 594 de 2000. "Ley General de Archivo" información electrónica de entidades públicas;"
- d) Ley 1150 de 2007. "Seguridad de la información electrónica en contratación en línea".
- e) Ley 1266 de 2008. "Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
- f) Ley 1273 de 2009. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Art. 199. Espionaje; Art. 258. Utilización indebida de información; Art. 418. Revelación de Secreto; Art. 419. Utilización de asunto





- sometido a secreto o reserva; Art. 420. Utilización indebida de información oficial; Artículo 431. Utilización indebida de información obtenida en el ejercicio de la función pública; Artículo 463. Espionaje.
- g) Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”.
 - h) Ley 1437 de 2011. “Procedimiento Administrativo y aplicación de criterios de seguridad”.
 - i) Ley 1480 de 2011. “Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas”.
 - j) Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la Protección de Datos Personales”.
 - k) Decreto Ley 019 de 2012. “Racionalización de trámites a través de medios electrónicos. Criterio de seguridad”.
 - l) Ley 1712 de 2014. “Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
 - m) Ley 1753 de 2015, Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país” en el artículo 45 establece: “Estándares, modelos y lineamientos de tecnologías de la información y las comunicaciones para los servicios al ciudadano”.

3. Decretos:

- a) Decreto 1727 de 2009. “Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información”.
- b) Decreto 2952 de 2010. “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”.
- c) Decreto 2364 de 2012. “Firma electrónica”.
- d) Decreto 2609 de 2012. “Expediente electrónico”.
- e) Decreto 2693 de 2012. “Gobierno electrónico”.
- f) Decreto 1377 de 2013. “Por el cual se reglamenta parcialmente la Ley 1581 de 2012”.
- g) Decreto 1510 de 2013. “Contratación pública electrónica”.
- h) Decreto 886 de 2014. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- i) Decreto 1083 de 2015. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- j) Decreto 415 de 2016. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2011 definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones”.
- k) Decreto 1008 de 2018, se define la política de Gobierno Digital, por el cual se establecen los lineamientos generales de la política de Gobierno Digital,





la cual tiene por objeto promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

4. Otras:

- a) CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- b) CONPES 3854 de 2016 Política Nacional de Seguridad digital.

Artículo 5. Definiciones.

De conformidad con la vigencia sobre la materia, se establecen las siguientes palabras contenidas en la Política Integral de Tecnologías de la Información de la Universidad Simón Bolívar, las cuales serán aplicadas e implementadas acogiendo los criterios de interpretación que garanticen una aplicación sistemática e integral. De tal forma, que deberán entenderse en el siguiente sentido:

1. **Activos de información.** Es el elemento de información que se recibe o produce en el ejercicio de sus funciones. Y se pueden definir en los siguientes ámbitos, y características internas:

Digitales

- Correos electrónicos
- Copias de seguridad
- Bases de datos
- Ecommerce
- Dispositivos de almacenamiento
- Servicios web
- Infraestructura digital

Tangibles

- Personas
- Financieros
- Legales
- Estrategia y comerciales
- Otros medios de almacenamiento

Intangibles

- Conocimiento de información
- Relacionamiento
- Licencias
- Conocimientos técnicos
- Imagen corporativa
- Marca
- Reputación Institucional
- Confianza de los interesados





Ética

Operativos

Servidores
Computadores
Dispositivos de red
Dispositivos de mano e incrustados
La nube

Servicios TI

Hardware
Enlaces
Dispositivos de comunicación
Tecnología
Administración de procesos
Software

2. **Arquitectura de TI.** Describe la estructura y las relaciones de todos los elementos de TI de una organización. Se descompone en arquitectura de información, arquitectura de sistemas de información y arquitectura de servicios tecnológicos. Incluye además las arquitecturas de referencia y los elementos estructurales de la estrategia de TI (visión de arquitectura, principios de arquitectura, lineamientos y objetivos estratégicos).
3. **Bienes.** Todo hardware o software que se defina dentro de las necesidades de la Institución.
4. **Confidencialidad.** Característica de la información que está disponible solo para personas o sistemas autorizados.
5. **Catálogo de Servicios de TI.** Es un inventario detallado y documentado de los servicios de TI que la institución tiene implementados y que se encuentran activos, incluyendo los que están disponibles para ser desplegados. El catálogo de servicios de TI es el subconjunto del portafolio de servicios publicado para los usuarios.
6. **CobIT - Control Objectives for Information and related Technology.** (Objetivos de Control para la información y Tecnologías Relacionadas): Publicados y mantenidos por ISACA, sus siglas en inglés (Information System Audit And Control Association) – Asociación de Auditoría y Control de Sistemas de Información Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser empleados por la alta dirección de las organizaciones y los auditores.
7. **Componente de información.** Es el término agrupador utilizado para referirse al conjunto de los datos, entidades de negocio, unidades de información, los servicios de





información y los flujos de información bajo un único nombre.

8. **Colaborador.** En el presente documento se emplea para referirse a directivos, funcionarios, docentes, contratistas, estudiantes, proveedores, colaboradores y visitantes de la Universidad Simón Bolívar, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la institución.
9. **Cultura, ética y comportamiento.** Es el conjunto de creencias, ideas, prácticas y comportamientos, individuales y colectivos.
10. **Dato.** Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.
11. **Dominio.** Son las dimensiones desde las cuales se debe abordar la gestión estratégica de TI.
12. **Disponibilidad.** Característica de la información a la cual solo pueden acceder personas autorizadas.
13. **Estrategia de TI.** Es el conjunto de principios, objetivos y acciones concretas que reflejan la forma en la cual una institución decide utilizar las Tecnologías de la Información para permitir el logro de su misión de una manera eficaz. La Estrategia TI busca alinearse como parte integral de la estrategia de una Institución.
14. **Gestión de TI.** Es una práctica o proceso, que permite operar, innovar, administrar, desarrollar y usar apropiadamente las tecnologías de la información (TI), con el propósito de agregar valor para la organización. La gestión de TI permite a una organización optimizar los recursos, mejorar los procesos de negocio y de comunicación y aplicar las mejores prácticas.
15. **Gobierno de TI.** Conjunto de acciones que realiza el área de TI en coordinación con la alta dirección para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio. El gobierno de TI gestiona y controla los riesgos, mide el desempeño de TI, busca optimizar las inversiones de TI y establecer un esquema de toma de decisiones de TI. El gobierno de TI es parte del gobierno corporativo o empresarial.
16. **Indicador.** Medida de logro de algún objetivo planteado.





17. **Información.** Es un conjunto de datos organizados y procesados que tienen un significado, relevancia, propósito y contexto. Ley 1712 /2014.
La Constitución de 1991, artículo 74 que “Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley”. Y bajo este mismo entendido la Ley 1712 de 2014 estableció en su artículo 2 que “Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente ley”
18. **Información Pública.** Es toda información que un sujeto obligado genere, obtenga adquiera, o controle en su calidad de tal. Ley 1712/2014 que ha sido declarada legalmente o por su propietario, de conocimiento público y accesible a cualquier persona.
19. **Información confidencial.** Es toda aquella información que tiene establecido tal carácter debido a leyes especiales en el marco Jurídico colombiano, que vulnere, afecte o atente contra los siguientes aspectos, Estrategias del Negocio, Competitividad, Expansión, Historias Clínicas, Ubicación Geográfica Específica, Secreto Profesional, entre otros.
20. **Información Secreta.** Es toda aquella información que tiene establecido tal carácter debido a leyes especiales en el marco jurídico colombiano, que vulnere, afecte o atente contra los siguientes aspectos, Actuaciones Políticas, Defensa Nacional y Seguridad del Estado, Políticas Monetaria, Investigación de Delitos, Material Clasificado e Información Registral.
21. **Información Pública Clasificada.** Es aquella información que estando en poder custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley; Ley 1712/2014.
22. **Información Pública Reservada.** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley; Ley 1712/2014.
23. **Información Semi-Privada.** Es aquella que por versar sobre información personal o impersonal y no estar comprendida por la regla general anterior, presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento





de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones

24. **Integridad.** Característica de la información que es modificada sólo por personas o sistemas autorizados y de una forma permitida.
25. **Interoperabilidad.** Habilidad de transferir y utilizar información de manera uniforme y eficiente entre varias organizaciones y sistemas de información. Habilidad de dos o más sistemas (computadoras, medios de comunicación, redes, software y otros componentes de tecnología de la información) de interactuar y de intercambiar datos de acuerdo con un método definido, con el fin de obtener los resultados esperados. El ejercicio de colaboración entre organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio, con el propósito de facilitar la entrega de servicios en línea a ciudadanos, empresas y a otras entidades. (Marco de Interoperabilidad para el Gobierno en línea).
26. **Obsolescencia Tecnológica.** Hace referencia a la necesidad de recambio de un aparato tecnológico simplemente por el hecho de que aparece una nueva versión del mismo, incluso aunque los cambios no sean significativos, ni el producto anterior haya llegado al final de su vida útil.
27. **PETI (Plan Estratégico de Tecnologías de la Información).** Es el artefacto que se utiliza para expresar la Estrategia de TI. Incluye una visión, unos principios, unos indicadores, un mapa de ruta, un plan de comunicación y una descripción de todos los demás aspectos (financieros, operativos, de manejo de riesgos, etc.) necesarios para la puesta en marcha y gestión del plan estratégico. El PETI hace parte integral de la estrategia de la institución. Cada vez que una Institución hace un ejercicio o proyecto de Arquitectura Empresarial, su resultado debe ser integrado al PETI.
28. **Plan De Calidad.** Es una directriz u orientación que tiene el propósito de establecer pautas para lograr los objetivos propuestos en la Estrategia de TI
29. **Política De TI.** Es una directriz u orientación que tiene el propósito de establecer pautas para lograr los objetivos propuestos en la Estrategia de TI. Son instrumentos para traducir el comportamiento deseado por la alta dirección en orientaciones prácticas para el día a día de la gestión
30. **Roles.** Conjunto de responsabilidades y actividades asignadas a una persona o grupo de personas para apoyar la adopción y aplicación del Marco de Referencia de Arquitectura Empresarial para la gestión de TI.
31. **Servicio de información.** Consiste en la entrega de información de valor para los usuarios de una Institución a través de un proveedor de servicio interno o externo. Un





servicio de información se describe a través de un contrato funcional (qué recibe como entrada y qué produce como salida) y un conjunto de acuerdos de servicio que debe cumplir.

32. **Servicio de TI.** Es una facilidad elaborada o construida usando tecnologías de la información para permitir una eficiente implementación de las capacidades institucionales. A través de la prestación de estos servicios es que TI produce valor a la organización. Los servicios de información son casos particulares de servicios de TI. Los servicios de TI deben tener asociados unos acuerdos de nivel de servicio.
33. **Tecnologías de la Información y las Comunicaciones – TIC.** Son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes.
34. **Tecnología Disruptiva.** Tecnología disruptiva o innovación disruptiva es aquella tecnología o innovación que conduce a la aparición de productos y servicios que utilizan preferiblemente una estrategia disruptiva (de disruptivo, 'que produce ruptura brusca') frente a una estrategia sostenible a fin de competir contra una tecnología dominante, buscando una progresiva consolidación en un mercado
35. **TI.** Tecnologías de la Información.
36. **Transformación Digital.** La transformación digital es la reinención de una organización a través de la utilización de la tecnología digital para mejorar la forma en que se la organización se desempeña y sirve a quienes la constituyen. Digital se refiere al uso de la tecnología que genera, almacena y procesa los datos para conseguir esa reinención.

Artículo 6. Política Integral de Tecnologías de la Información.

Se define la política Integral de TI como la manifestación estratégica institucional para establecer las pautas, directrices y orientaciones que regulen el comportamiento de los usuarios y la forma de gobernar y gestionar de manera adecuada y efectiva los esquemas de Estrategia TI, Gobierno TI, Información, Sistemas de Información, Servicios Tecnológicos, Uso y Apropiación.

Artículo 7. Principios activos de la política Integral de TI

La política de TI en la Universidad Simón Bolívar se basará en los siguientes principios activos, que dentro del marco de referencia de arquitectura empresarial determinará la aplicabilidad en 5 dominios al momento de tomar decisiones, según las directrices u orientaciones dadas.





1. **El dato es un activo y se gobierna:** Los datos de la Universidad Simón Bolívar son activos intangibles de muy alto valor y como tal se les debe proveer el tratamiento correspondiente a la recolección, uso, gestión y suministro preciso y oportuno de los mismos.
2. **El dato público es compartido:** los datos de la Universidad Simón Bolívar que estén clasificados como públicos, deben ser compartidos para lograr mayor eficiencia en los procesos como muestra de transparencia y de buen gobierno institucional.
3. **El dato es accesible:** los datos de la Universidad Simón Bolívar se deben encontrar a disposición de quienes requieran acceder a ellos, grupos de interés, procesos o aplicaciones.
4. **Calidad de los datos:** los datos deben ser completos, exactos, responder con veracidad a la situación actual de la Institución, ser aptos para su uso y cumplir con el conjunto de atributos relevantes de calidad de datos definido.
5. **Seguridad de la información:** la información debe ser clasificada y protegida contra la divulgación y uso no autorizado.
6. **Alineación de TI con los objetivos estratégicos:** los planes y proyectos en tecnologías de la información y las comunicaciones deben estar orientados al cumplimiento de la misión, los objetivos estratégicos de la Universidad Simón Bolívar y satisfacer las necesidades derivadas de la estrategia misional.
7. **Interoperabilidad y colaboración:** los procesos de la Universidad Simón Bolívar deben compartir datos y posibilitar el intercambio de información entre ellos, con otras instituciones y con los colaboradores. La interoperabilidad es necesaria y prioritaria para la cooperación, desarrollo, integración y prestación del servicio a nuestros beneficiarios, mejorar los procesos internos y dar cumplimiento a la Ley.
8. **Uso eficiente de los recursos de TI:** La Universidad Simón Bolívar debe establecer mecanismos para el uso eficiente de los recursos de tecnología. Las adquisiciones se deben hacer en razón a la priorización de necesidades, con base en análisis adecuados y permanentes. La dirección de TI debe estar dimensionada para dar soporte a la organización, proporcionando servicios con calidad.
9. **Servicios compartidos de infraestructura:** La Universidad Simón Bolívar debe centralizar las actividades comunes, economizando en recursos humanos, infraestructura, incrementando el mejoramiento del servicio, así mismo contar con





una infraestructura tecnológica centralizada, estandarizada y dimensionada para dar soporte a toda la Institución.

10. **Disponibilidad de la infraestructura de TI:** la infraestructura de hardware, software y telecomunicaciones debe estar en funcionamiento y al servicio de los usuarios internos y externos cuando lo requieran.
11. **Uso y apropiación de soluciones TI:** las iniciativas de TI deben contar con estrategias de uso y apropiación que promuevan las buenas prácticas para el correcto uso y aprovechamiento de las soluciones de TI que aportan a los procesos de la Institución.

Artículo 8. Dominios.

Al establecer y detallar los principios activos para los dominios de arquitectura empresarial de la Universidad Simón Bolívar conforme a los marcos de referencia MINTI-IT4+ (Estrategia TI, Gobierno TI, Información, Sistemas de información, Servicios tecnológicos, Uso y apropiación) se da cumplimiento a la normatividad vigente y se aporta al logro de los objetivos estratégicos de la Universidad Simón Bolívar. En lo cual se define y detalla a continuación.

1. **ESTRATEGIA TI.** La Institución dentro de su estrategia TI en cabeza de la Dirección de TI y en colaboración de las áreas funcionales, debe alinear su estrategia a su plan estratégico de desarrollo, logrando adaptabilidad, valor, eficiencia y logro de sus objetivos. En ese sentido, a través de la Dirección de TI se definen de las siguientes políticas.
 - a) Impulsar la creación y/o actualización de un plan estratégico de las tecnologías de la Información, el cual contribuya con el logro de los objetivos estratégicos y así generar valor con el fin de cumplir las necesidades que se derivan de la misión institucional. Esto deberá ser aceptado, comprendido y actualizado continuamente.
 - b) Organizar los proyectos de inversión en tecnología de forma que sea definidas por su estructura, formulación, diseño y evaluación a fin de seguir las directrices de la Vicerrectoría Financiera y la Dirección de Planeación de la institución.
 - c) Identificar estándares y/o políticas que faciliten la gestión y gobernabilidad de TI, contemplando temas como seguridad, continuidad de negocio, gestión de información, adquisición tecnológica, desarrollo e implementación de sistemas de información, acceso a la tecnología, y uso y apropiación por parte de los colaboradores.
 - d) Definir evaluaciones periódicas por medio de los indicadores de la estrategia que permitan determinar avances y cumplimientos establecidos en el PETI de la Universidad Simón Bolívar.
 - e) Participar en la concepción, planeación y desarrollo de los proyectos de la institución donde se tenga en cuenta ítems asociados a tecnología de información, dentro de los lineamientos definidos por las coordinaciones y áreas funcionales, a favor de buscar soluciones que favorezcan el crecimiento y desarrollo de estas.





- f) En el ejercicio de las funciones de la Dirección de Tecnologías de la Información, alineada con el marco de referencia de arquitectura empresarial; debe mantener un trabajo articulado con la alta dirección que permita ser transversal en las áreas funcionales de la institución.
 - g) Realizar seguimiento y control del presupuesto y el plan de compras asociados a los proyectos estratégicos definidos en el PETI, los Planes de Acción, el Plan Estratégico de Desarrollo y los Planes de Mejoramiento de la institución.
 - h) La proyección del plan estratégico de TI deberá estar alineado en tiempo con el -PED- y ser actualizado según las condiciones que se presenten, a nivel de cambios, correcciones o actualizaciones de la normatividad y tendencias tecnológicas de la industria.
 - i) Tener un plan de comunicación de las estrategias, políticas, proyectos, resultados y servicios a las partes interesadas de la Institución referente a temas de Tecnologías de la información.
 - j) Diseñar, estructurar y actualizar el catálogo de servicio de TI de la Universidad Simón Bolívar a fin de mantener los acuerdos de niveles de servicios (ANS) asociados.
2. **GOBIERNO TI.** El gobierno de TI en cabeza de la Dirección de TI y áreas funcionales estructurara las relaciones y procesos destinados con fin de dirigir y alcanzar sus objetivos para añadir valor mientras se equilibran los riesgos y el retorno de las TI y sus procesos. En ese sentido, a través de la Dirección de TI se definen de las siguientes políticas.
- a) Definir y tener implementado un esquema de gobierno de TI en forma de comité, alineado al modelo integrado de planeación y gestión que incluya: proceso de gestión de TI, indicadores de desempeño de TI, instancias de decisiones de TI definidas, estructura organizacional del área de TI, para definir las roles y responsabilidades que le competen a cada uno de los funcionarios y usuarios de la Institución y así se asegure una adecuada segregación de funciones para garantizar la protección adecuada de la información.
 - b) Definir una política de TI acorde con su contexto y misión, la cual tiene que ser aprobada por la sala general; debe ser implementada y actualizada según la necesidad.
 - c) Tener indicadores y mediciones de desempeño de la gestión de TI a través de tableros de control. Formular acciones de mejoras a partir de los resultados de dichos indicadores.
 - d) Garantizará que cualquier iniciativa o plan de la Institución que incorpore Tecnologías de la Información según la necesidad o circunstancia que lo amerite, será liderado en conjunto entre las áreas misionales y el proceso de gestión de TI, incorporándose desde el inicio del proyecto.
 - e) Aplicar metodologías y criterios de evaluación para la selección de alternativas de solución tecnológica, antes de realizar inversión en TI. Utilizará acuerdos de marcos de precio y contrato para adquisición de bienes y/o servicio.





- f) Tener metodología para la gestión de proyectos de TI, y realizar actividades de transferencia de conocimiento, desde gestores de TI, directivos, funcionarios, Profesores, contratistas, estudiantes, proveedores, colaboradores y visitantes.
- g) La Coordinación de Seguridad Informática y la Coordinación de Proyectos TI podrán realizar auditorías para verificar el seguimiento de los proyectos o actividades de las Coordinaciones adjuntas a la Dirección de Tecnologías de la Información en base a lineamientos de la norma de Seguridad de la Información ISO 27001, según sea el enfoque que se determine tratar.

3. **INFORMACION.** Para la Universidad Simón Bolívar, el dominio de información, es fundamental en su uso, apoyando eficientemente a las áreas funcionales en la toma de decisiones, a fin de generar valor a la institución y colaboradores. Donde se garantice la transparencia, trazabilidad y seguridad en el ciclo de vida de la información. De lo anterior se definen las siguientes políticas.

- a) Definir las directrices y liderazgo en la gestión de los datos durante su ciclo de vida, desde que se ingresa a los sistemas de información, se procesa y se obtienen los resultados definidos, articulando personas, procesos y tecnología involucrados como activos de información de la Institución.
- b) Contar con un plan de calidad que les asegure a los procesos de la Institución, que la información va a ser controlada e inspecciona a fin de mantener indicadores que permitan realizar acciones preventivas, correctivas y/ mejoramiento continuo.
- c) Los datos personales como información vital de los directivos, funcionarios, profesores, contratistas, estudiantes, proveedores, colaboradores y visitantes, será utilizada para el procesamiento de los requerimientos contractuales que se tenga con la institución, tales como documentos de identidad, fotos, y exime de responsabilidad legal su uso, salvo que esta no sea utilizada para los fines para los cuales fue dispuesta.
- d) Se debe tener presente que no todas las fotografías son un dato personal; solo lo serán aquellas en las que se permita establecer la identidad de una o varias personas naturales en particular. Y que, así mismo, para la recolección y uso de fotos como Datos Personales Sensibles deben observarse las reglas especiales señaladas en el artículo 6 del Decreto 1377 de 201317 en concordancia con lo dispuesto en los artículos 9 y 12 de la Ley Estatutaria 1581 de 2012.
- e) En materia de tratamiento y protección de datos personales, deberá tener consignada una política con todos los apartes que involucre el cumplimiento como anexo del manual de funciones sustantivas de institución.
- f) Mantener trazabilidad de la información en los procesos establecidos de la Universidad, a fin de fortalecer la no obtención de hallazgos y no conformidades realizadas por los sistemas de gestión y calidad con mecanismos de auditoría.
- g) Basar el principio de interoperabilidad a fin de compartir datos alojados en los sistemas de información de la institución con otras instituciones o entidades del estado a partir de las necesidades del intercambio de información a través de la tecnología de la información.





- h) La información debe ser clasificada en función de su valor, sensibilidad y criticidad para la Institución, con el fin de determinar el grado de protección requerida al ser manipulada.
- i) Definir un método para la clasificación de la información donde se definan las categorías a utilizar. Para esta definición se deben tomar en cuenta las diferentes Instancias Directivas de la institución.
- j) El método de clasificación de la información debe considerar información impresa o digital, independientemente del tipo de almacenamiento o medio de transferencia.
- k) La Dirección de Tecnologías de la Información en una labor conjunta con las Instancias Directivas de la institución, deben definir revisiones periódicas del método de clasificación de la información.
- l) Desarrollar los procedimientos establecidos para la revisión del método de clasificación de la información, los cuales deben incluir la valoración de las necesidades de la Institución para compartir y restringir la información, las obligaciones legales en caso de que existan y el nivel de impacto asociado.
- m) En los servicios de intercambio de información, se debe cumplir con las condiciones de seguridad, calidad y el tratamiento confidencial que aplique. La Institución debe implementar las medidas de seguridad en la transmisión y entrega de la información. Se deben acatar los acuerdos de confidencialidad para salvaguardar la información que así lo requiera y proporcionar las condiciones de almacenamiento de la información intercambiada.
- n) Cuando se suscriban acuerdos con otras organizaciones que compartan información con la institución deben incluir procedimientos para identificar la clasificación de dicha información e interpretar la marca de clasificación de otras organizaciones.
- o) Proporcionar las estructuras, Tecnologías y herramientas de bases de datos, que son quienes traducen las necesidades de los dueños de los datos en requisitos tecnológicos. Así mismo, la Institución debe tener definidas las responsabilidades de todos los actores que intervienen en la gestión de los datos y de la información institucional.
- p) Los gestores de TI, directivos, funcionarios, Profesores, contratistas, estudiantes, proveedores, colaboradores y visitantes deben valorar el rol estratégico de la información; y ser conscientes de los datos y la información a su cargo, así como de los procesos de la Institución que los crean, almacenan, procesan y utilizan, reconociendo que son de propiedad de la Institución.
- q) Se debe contar con las condiciones institucionales que permitan brindar un adecuado nivel de acceso a los datos en cualquiera de sus clasificaciones; los accesos se permiten de forma segura, con niveles de acceso, salvaguardando las responsabilidades y autonomía de la Institución en cuanto a la accesibilidad, mantenimiento y actualización de los datos.
- r) Se deben tener identificados e implementados los medios y canales apropiados para brindar mecanismos de acceso a los datos; las consultas y accesos a datos públicos que son gratuitos. Se debe realizar monitoreo, identificar oportunidades de mejora y optimizar los mecanismos de acceso para los actores que puedan consultar los datos.





Se debe disponer de sistemas de información efectivos que le permiten al usuario un fácil acceso a la información.

- s) La Institución debe mantener la capacidad para recuperar los datos perdidos luego de un incidente. Deben existir procedimientos para la realización de copias de seguridad que garanticen la recuperación de la información. Según el nivel de criticidad de la información y los volúmenes de información a copiar, se deben aplicar las tecnologías adecuadas, el esquema de respaldo, la frecuencia y el soporte utilizado. Las copias de respaldo deben ser planificadas. Se deben tener definidos y aplicar los mecanismos de comprobación para verificar el estado de la copia. Los medios deben ser guardados en un sitio seguro. Se debe probar periódicamente la confiabilidad del sistema de respaldo.

4. **SISTEMAS DE INFORMACION.** Los sistemas de información y aplicaciones son el soporte tecnológico de los procesos de la Universidad Simón Bolívar. Por lo que esto permitirá planear, diseñar la arquitectura, el ciclo de vida, las aplicaciones, los soportes y la gestión de los sistemas que facilitan y habilitan las dinámicas en la institución. De lo anterior se definen las siguientes políticas:

- a) La Dirección de Tecnologías de la Información dispondrá un catálogo consolidado y actualizado de sus sistemas de información, que incluya atributos que permitan identificar la información relevante que facilite la gobernabilidad de estos.
- b) Incorporar en el diseño de los sistemas de información aquellos componentes de seguridad alineados con la normativa establecida que incluyan, como mínimo: el tratamiento de la privacidad de la información, la implementación de controles de acceso (autorización y autenticación) así como los mecanismos de integridad y cifrado de la información.
- c) Las Coordinaciones adjuntas a la Dirección de Tecnologías de la Información deberán establecer y utilizar una metodología formal para el desarrollo y mantenimiento de software, que oriente los proyectos de construcción o evolución de los sistemas de información que se desarrollen a la medida, ya sea internamente o a través de terceros.
- d) Los productos digitales basados en desarrollo de software nuevos o existentes deben ser trazables, estar documentados y desarrollarse en ambiente web. Cuando se suscriban contratos con terceras partes bajo la figura de "obra creada por encargo" o similar, cuyo alcance incluya el desarrollo de elementos de software, la institución debe incluir en dichos contratos, la obligación de transferir a la institución los derechos patrimoniales sobre los productos desarrollados. Se debe cumplir con las políticas de seguridad e interoperabilidad. Los sistemas de información deben ser sujetos de auditorías de calidad y funcionalidad de manera periódica.
- e) La Dirección de Tecnologías de la Información en conjunto a las coordinaciones adjuntas de la Universidad Simón Bolívar debe identificar y mantener la independencia de los ambientes requeridos durante el ciclo de vida de los sistemas de información, ya sea directamente o través de un tercero. Ejemplos de ambientes son: desarrollo, pruebas, capacitación, producción.





- f) La Dirección de Tecnologías de la Información debe garantizar que, dentro del proceso de desarrollo de sistemas de información, se ejecuten estrategias de integración continua sobre los nuevos desarrollos de sistemas de información y productos digitales.
- g) En el proceso de desarrollo y evolución de un sistema de información, la Dirección de Tecnologías de la Información debe contar con un plan de pruebas que cubra los requerimientos funcionales y no funcionales. La aceptación de cada una de las etapas de este plan debe estar vinculada a la transición del sistema de información a través de los diferentes ambientes.
- h) La Dirección de Tecnologías de la Información debe realizar constantemente capacitación y entrenamiento funcional y técnico a los colaboradores, con el fin de fortalecer el uso y apropiación de los sistemas de información.
- i) La Dirección de Tecnologías de la Información debe asegurar que todos sus sistemas de información cuenten con la documentación técnica y funcional debidamente actualizada.
- j) La Dirección de Tecnologías de la Información debe garantizar que todos los cambios en los sistemas de información se encuentran debidamente documentados y soportados en el procedimiento para el control de cambios para los sistemas de información de la institución.
- k) Para el mantenimiento de los sistemas de información, la Dirección de Tecnologías de la Información debe hacer un análisis de impacto ante cualquier solicitud de cambio en alguno de sus componentes, con el fin de determinar la viabilidad del cambio y las acciones a seguir.
- l) La Dirección de Tecnologías de la Información debe establecer criterios de aceptación y definir Acuerdos de Niveles de Servicio (ANS) cuando se tenga contratado con terceros el mantenimiento de los sistemas de información. Los ANS se deben aplicar en las etapas del ciclo de vida de los sistemas de Información que así lo requieran y se debe velar por la continuidad del servicio.
- m) Durante todas las fases del ciclo de vida de los sistemas de información, la Coordinación de Desarrollo de Software debe analizar e incorporar aquellos componentes de seguridad y privacidad de la información que sean necesarios.
- n) La Dirección de Tecnologías de la Información en conjunto a las Coordinaciones adjuntas debe desarrollar mecanismos que aseguren el registro histórico de las acciones realizadas por los colaboradores sobre los Sistemas de Información, manteniendo la trazabilidad y apoyando los procesos de auditoría.
- o) Los Sistemas de Información que estén disponibles para el acceso a los colaboradores o aquellos que de acuerdo con la caracterización de colaboradores lo requieran, deben cumplir con las funcionalidades de accesibilidad.
- p) La dirección de TI debe asegurar que en el diseño e implementación de sus sistemas de información se incorporen funcionalidades que faciliten la generación de datos abiertos. Así mismo, se deben automatizar los procesos de extracción de los sistemas de información, fuente para la generación y publicación de conjuntos de datos abiertos.





- q) La Dirección de Tecnologías de la Información propenderá por garantizar que todos los sistemas de información consignados en el inventario de software se encuentren correctamente licenciados y actualizados a sus últimas versiones, así como de mantener los contratos de soporte y mantenimiento para aquellos de uso especializado.
- r) Antes de optar por la adquisición de un nuevo software, se debe revisar el alcance de las plataformas institucionales y validar si alguna de ellas cuenta con la funcionalidad para suplir el requerimiento, además es necesario determinar la viabilidad de un desarrollo dentro de la misma, que permita optimizar los recursos institucionales.
- s) La Dirección de Tecnologías de la Información es la encargada de emitir concepto técnico de los requerimientos de software que se originen en la institución.
- t) Asegurar que los problemas e incidentes presentados en sistemas de información y plataforma tecnológica sean resueltos y que sus causas sean investigadas para mitigar su recurrencia.

5. **SERVICIOS TECNOLOGICOS.** Para la Universidad Simón Bolívar es de vital importancia garantizar la eficacia, estándares de calidad, optimización de recursos y transparencia en los servicios e infraestructura tecnológica ofrecidos a la comunidad institucional.

De lo anterior se definen las siguientes políticas.

- a) Se garantizará la operación de servicios de Tecnología de la Información subcontratados para mantener la protección de la información de la institución y la confiabilidad de la prestación de servicios.
- b) La Dirección de Tecnologías de la Información debe realizar actividades de evolución, mantenimiento y optimización de la plataforma tecnológica para la prestación y consumo de servicios de intercambio de información.
- c) Se mantendrá constante monitoreo de la infraestructura de TI y los eventos relacionados, almacenando suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las otras actividades que rodean o respaldan las operaciones.
- d) Se llevará un registro actualizado de todos los elementos que configuran la infraestructura de Tecnologías de la Información junto con sus interrelaciones: dispositivos de hardware, software y documentación. Para cada elemento debe tener asociados sus atributos relevantes. Se debe conocer el estado de cada componente en todo momento durante su ciclo de vida.
- e) Se mantendrán medidas de protección contra factores ambientales, instalando equipos y dispositivos especializados para monitorear y controlar el medio ambiente en el Datacenter de la Institución.
- f) Se deberá identificar, registrar y clasificar las solicitudes e incidentes de servicio, y asignar una prioridad de acuerdo con los ANS establecido por la Dirección de Tecnologías de la Información en conjunto a la Coordinación de Soporte Técnico.





- g) Siempre que la Institución plantee la adquisición, desarrollo o adaptación de una solución informática, se debe concebir que los datos que administrará la aplicación en cuestión sean intercambiados con otras aplicaciones de la misma Institución o con otras Instituciones en el futuro. Por principio general, todo sistema de información debe ser susceptible de intercambiar la totalidad o al menos una parte de su información con otros sistemas de información, así esto no sea una necesidad manifiesta en el primer momento en el que se construye la solución Tecnológica. aplicación. Por esto, ante el desarrollo de cada aplicación, se deben fijar las pautas específicas que dictan qué información será capaz de compartir y cómo lo logrará. Se debe evaluar qué funcionalidades de integración con otras aplicaciones ofrecerá la aplicación, considerando el cumplimiento de los atributos de calidad de los datos y las políticas de calidad. Las aplicaciones deben ser diseñadas de tal manera que garanticen la interoperabilidad, una de las verificaciones se evidencia con la obtención de la certificación de lenguaje común de intercambio de información que permite estandarizar los datos a intercambiar
- h) Se contará con un catálogo de servicios de información, que le permita a la institución administrar, analizar y mejorar los activos de Tecnologías de la Información de la Institución.
- i) La Universidad Simón Bolívar podrá contratar cualquier tipo de servicios especializados de tecnología (tales como Servicios Cloud, IaaS, PaaS, SaaS, etc) así como desarrollar los proyectos que sean necesarios, que permitan el reforzamiento de los lineamientos estratégicos institucionales.
- j) Se establecerá y mantendrá un plan para permitir a la institución, en función a las Tecnologías de la Información, responder a los incidentes e interrupciones para continuar con la operación de los procesos críticos y servicios de TI, a fin de mantener disponibilidad a nivel aceptable en la institución. Esto se definirá dentro del procedimiento de seguridad de la información, con relación a los planes de gestión de la continuidad del negocio y Planes de Recuperación de Desastres DRP.
- k) Se deberá mantener alta disponibilidad de los servicios tecnológicos aumentando las capacidades de alta disponibilidad de la infraestructura crítica de la Institución, estas deben ser puestas a prueba periódicamente para garantizar la ejecución de la funcionalidad de los DATACENTER de respaldo.
- l) La Dirección de Tecnologías de la Información tendrá a bien contratar los servicios de interconexión a redes externas tales como Internet dedicado, banda ancha, MPLS o cualquier otro similar, que este alineado con los objetivos institucionales y que permita la institución fortalecer los servicios ofrecidos a la comunidad académica.
- m) La Dirección de Tecnologías de la Información, en conjunto a la coordinación de soporte técnico deberá velar por los cumplimientos de los acuerdos de servicios de (ANS), a fin de garantizar cumplimiento a los directivos, funcionarios, Profesores, contratistas, estudiantes, proveedores, colaboradores y visitantes.
- n) Los servicios de Tecnologías de la Información, prestados internamente o por empresas externas se deben ejecutar contra acuerdos de niveles de servicios - ANS equitativos, exigibles y a un costo razonable. La calidad de los servicios debe ser





- monitoreada respecto de los objetivos establecidos en los Acuerdos de Nivel de Servicio.
- o) La Dirección de Tecnologías de la Información, en conjunto a sus Coordinaciones adjuntas seguirá lineamientos para atender los requerimientos de soporte de primer, segundo y tercer nivel, para sus servicios de TI, a través de un punto de contacto por medio de la herramienta de GLPI de la mesa de ayuda.
 - p) Garantizar la renovación constante y eficaz de los equipos que soportan las TI en la Universidad Simón Bolívar, indispensables para el buen desempeño de las actividades misionales y la adecuada prestación del servicio a toda la comunidad (gestores de TI, directivos, funcionarios, Profesores, contratistas, estudiantes, proveedores, colaboradores y visitantes), proporcionando los elementos tecnológicos necesarios para que las diferentes áreas de la Universidad presten un mejor servicio, sea a través de los equipos de cómputos institucionales, los servidores del centro de datos y de comunicaciones para brindar un servicio óptimo y permanentemente con alta disponibilidad dentro y fuera del campus universitario.
 - q) Debe existir un punto de contacto entre los usuarios y la Dirección de TI que atienda las peticiones de los usuarios proporcionándoles información y acceso a los servicios, registre y monitoree los incidentes, aplique soluciones, realice la gestión de requerimientos, sea de fácil acceso para los usuarios y ofrezca servicios homogéneos y de calidad.
 - r) La Dirección de Tecnologías de la Información a través de sus Coordinación de Redes e Infraestructura Tecnológica deberá realizar y mantener copias de seguridad de la información de la Institución en medio digital, siempre que ésta sea reportada por el responsable de esta, con el objetivo de recuperarla en caso de cualquier tipo de falla, ya sea de hardware, software, o de procedimientos operativos al interior de la Institución.
 - s) Se deberá asegurar la implementación de un plan de mantenimiento preventivo, correctivo sobre la toda la infraestructura de la Institución y demás servicios tecnológicos coordinados por las dependencias adjuntas a la Dirección de TI.
 - t) Se deberá monitorear y controlar los niveles de consumos de los recursos que son compartidos por los servicios tecnológicos de la institución.
 - u) Las compras y adquisiciones de recursos de TI se deben realizar con base a necesidades reales y a requerimientos específicos, permitiendo alinear la inversión en Tecnologías de la Información a las metas institucionales; se deben definir prioridades institucionales en materia de compras y adquisiciones de TI, estableciendo niveles de gastos presupuestados y coherentes. Se deben realizar análisis costo – beneficio para la adquisición de nuevas soluciones, los cuales incluyan adicionalmente aspectos de seguridad de la información, riesgo y cumplimiento.
 - v) La Dirección de Tecnologías de la Información gestionara compras de tecnología (hardware y software), para lo cual se requieren al menos tres (3) cotizaciones comparables al mismo nivel técnico, exceptuando casos especiales donde el recurso sea ofrecido por un solo proveedor (exclusividad del producto por el proveedor o casa fabricante) o donde la infraestructura tecnológica requiera recursos de una marca o





proveedor específicos, lo cual debe estar debidamente justificado, así como también se debe establecer como obligatorio la adquisición de pólizas necesarias, velar por cubrir las necesidades de repuestos y mantenimiento de la infraestructura tecnológica. La adquisición de la infraestructura tecnológica se debe priorizar en los fabricantes con presencia en el país y capacidad de brindar soporte técnico garantizado. De igual manera, se pueden realizar adquisiciones por empresas distribuidoras nacionales e internacionales, debidamente autorizadas por los fabricantes y así poder garantizar el soporte técnico.

- w) Asegurar la adecuada evaluación y contratación de terceros que provean bienes y/o servicios relacionados con tecnologías de la información. Acerca de las compras y las solicitudes, la Dirección de TI incluirá dentro del plan de inversión de TI la compra de recursos tecnológicos utilizados en puestos de trabajo, para:
- Equipos de cómputo y herramientas tecnológicas destinadas al apoyo a las funciones misionales y de apoyo de la institución.
 - Reposición por daños de equipos adquiridos con fondos de la Universidad.
 - Dotación de puestos de trabajo para nuevos cargos de docentes o funcionarios o administrativos.
 - Las compras para renovaciones tecnológicas y dotaciones de puestos de trabajo para nuevos cargos, se realizará preferiblemente en el primer trimestre del año.
 - Las renovaciones y compra de nuevos equipos informáticos y de software de los laboratorios académicos se adquirirán con presupuesto de los departamentos académicos. Para el caso de proyectos de investigación y para las unidades de negocio de la Universidad los equipos se adquirirán de sus respectivos presupuestos.
 - La Dirección de Tecnologías de la información será la encargada de revisar las solicitudes de compras de recursos computacionales, en cuanto a la ubicación y conectividad (corriente regulada y red de datos) y definir las especificaciones técnicas requeridas.
 - Las compras de recursos computacionales se realizarán de acuerdo con las asignaciones presupuestales que tenga cada solicitud realizada.
 - Los proyectos de investigación anexarán a la solicitud de compra, el presupuesto detallado de las inversiones en recursos computacionales aprobadas por la vicerrectoría académica o vicerrectoría de investigación según corresponda y por la vicerrectoría financiera.
- x) Se deberá asegurar que la infraestructura y demás servicios tecnológicos de la institución cuenten con alertas tempranas ligadas a umbrales de operación que tengan definidos según las consideraciones de los administradores de los servicios, sistemas e infraestructura tecnológica y de información.
- y) Los equipos de cómputo y demás recursos tecnológicos destinados al apoyo de los procesos académicos y administrativos, no podrán tener un tiempo de uso superior a la garantía o soporte ofrecido por el fabricante. En cualquier caso, este tiempo no podrá ser superior a los 5 años contados a partir de la fecha de entrada en servicio, a





- menos que la adición de tiempo sea justificada y avalada por la Dirección de Tecnologías de la Información y certificada por el fabricante. Esto con el fin de evitar riesgos asociados a la obsolescencia tecnológica.
- z) Se deberá contar con mecanismos para el respaldo de los servicios críticos de la institución, así como un proceso periódico de respaldo de la configuración y la información almacenada en la infraestructura tecnológica, incluyendo información clave de las estaciones de trabajo de los colaboradores. Este proceso debe ser probado periódicamente y debe permitir la recuperación íntegra de los Servicios Tecnológicos.
 - aa) Se deberá contar con un Plan de recuperación de desastres y continuidad del negocio que tenga como objetivo definir los lineamientos en caso de interrupciones de los servicios tecnológicos de la institución.
 - bb) La Dirección de tecnologías de la Información, puede modificar o suspender los servicios tecnológicos de manera parcial o total a uno o varios de los directivos, funcionarios, docentes, contratistas, estudiantes, proveedores, colaboradores y visitantes, cuando se requiera por motivos de seguridad, por mantenimiento de los servicios preventivo o correctivo, por solicitud expresa de la alta dirección o por causas de fuerza mayor.
 - cc) La Dirección de Tecnologías de la Información será la única dependencia de la Institución con la capacidad de adquirir, desarrollar o avalar la adquisición y recepción de soluciones tecnológicas de cualquier tipo, conforme a los requerimientos de las diferentes dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de la plataforma tecnológica institucional. En consecuencia, cualquier solución tecnológica que opere en la Institución y no haya sido entregado a la Dirección de Tecnologías de la Información, no serán responsabilidad de esta, no se le brindará soporte y no se le salvaguardará la información.
 - dd) La Universidad Simón Bolívar implementará soluciones en tecnologías disruptivas basadas e innovaciones (Big Data, virtualización, modelos basados en analítica de datos, machine learning, Cloud, Blockchain, IoT, ciberseguridad), a fin de mejorar la aplicación de los sistemas de información y la prestación de servicios a los directivos, funcionarios, Profesores, contratistas, estudiantes, proveedores, colaboradores y visitantes.
 - ee) Se deberá documentar todos los procedimientos y caracterización de los procesos y/o servicios a fin de mantener información y ayudar a la transferencia de conocimientos a los colaboradores según la función que este tenga en la institución.
 - ff) Toda adquisición de infraestructura tecnológica debe estar contemplada en el plan de inversiones sustentado por el Plan de Acción de la Dirección de Tecnología de la Información, el PETIC, Plan Estratégico de Desarrollo y debe ejecutarse conforme a los procedimientos establecidos por la Universidad Simón Bolívar. No obstante, de acuerdo con las necesidades de la Universidad y con su debida justificación, será posible la adquisición de tecnología (Hardware o Software) que no estuviera inicialmente prevista.





- gg) La adquisición de nueva infraestructura tecnológica debe estar alineada al Plan Estratégico de Tecnologías de la Información enmarcado en el Plan Estratégico de Desarrollo institucional, que promueva la generación de valor.
 - hh) La Dirección de Tecnologías es la encargada de avalar técnicamente los requerimientos de Hardware y software que se originen en la institución.
 - ii) Para la adquisición es necesario tener en cuenta modelos de compras, leasing o renting según sea la necesidad o requerimiento del análisis que haya sido realizado conjuntamente con la vicerrectoría financiera.
 - jj) Ningún equipo de Infraestructura de Redes y Comunicaciones, cuyo objetivo sea de servicio misional, podrá tener un tiempo de uso superior a la garantía o soporte ofrecido por el fabricante. En cualquier caso, este tiempo no podrá ser superior a los 5 años contados a partir de la fecha de entrada en servicio, a menos que la adición de tiempo sea justificada y avalada por la Dirección de Tecnologías de la Información o certificada por el fabricante, esto con el fin de evitar riesgos asociados a la obsolescencia tecnológica.
 - kk) La Dirección de Tecnología de la información deberá realizar análisis en la elección de proveedores, con el fin de cumplir las condiciones mínimas que condicionen y beneficien los objetivos institucionales de la Universidad en torno a las TI.
 - ll) La Institución debe incentivar la eficiencia en el consumo de energía y de papel utilizando tecnologías respetuosas con el medio ambiente. Mediante métodos de computación en la nube, sistemas de teleconferencia, virtualización, optimización del centro de datos, impresión controlada, reciclaje y correcta disposición de equipos; la Institución demostrará conformidad con los lineamientos ecoeficientes. Se deben utilizar las TI como herramientas que facilitan el teletrabajo, reducen el impacto medioambiental y logran reducción de costos.
 - mm) Se deben determinar Acuerdos de Nivel operativo – ANO, conjuntamente con el proveedor para cada proyecto o servicio brindado por un tercero.
 - nn) Todo servicio tecnológico, debe incluir una estrategia de gestión del cambio organizacional que permita la gestión del impacto y los intereses de los usuarios de dicho servicio, que garanticen el uso y apropiación de este.
 - oo) La mesa de ayuda debe mantener informado a los usuarios solicitantes de la evolución de sus requerimientos. Si el requerimiento no puede ser implementado en los tiempos establecidos en los ANS, el usuario debe ser informado.
 - pp) La institución deberá implementar la disposición final de recursos tecnológicos, teniendo en cuenta los lineamientos técnicos con que cuente el gobierno, ya se para donación a entidades públicas o privadas según será su función.
6. **USO Y APROPIACION.** Para la Universidad Simón Bolívar es de vital importancia poder acercar y transmitir mediante estrategias, el uso y apropiación de los productos y servicios digitales y proyectos de TI, a fin de dinamizar el acceso de las tecnologías de la información socializando y sensibilizando en un marco de acciones que generen empatía con la cultura institucional en torno a las TI. De lo anterior se definen las siguientes políticas.





- a) La institución deberá asegurar que los colaboradores estén haciendo uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades asociados, realizando un plan completo de entrenamiento y desarrollo.
- b) Los recursos como correo electrónico, usuarios para acceder a sistemas de información y demás recursos tecnológicos, deben ser utilizados exclusivamente para las funciones contractuales que se hayan establecido con la Universidad.
- c) La responsabilidad ante acciones inadecuadas sobre el uso de los recursos tecnológicos que la Universidad provea a sus colaboradores podrá ser motivo de investigación en el caso que lo amerite, dando lugar a la aplicación de los procedimientos de control interno o externo según se determine.
- d) Se deberá trabajar en desarrollar las competencias de TI de los colaboradores, a fin de contribuir en el aumento de las capacidades de TI y la transformación requerida por la Universidad Simón Bolívar.
- e) Se deberán desarrollar estrategias de uso y apropiación a fin de motivar a los colaboradores en favor de las iniciativas de TI.
- f) Se deberán implementar indicadores que permitan evaluar el nivel de adopción de las TI y tomar las acciones de mejora por parte de la Institución a partir de los resultados obtenidos.
- g) La Dirección de TI, en conjunto de las áreas funcionales de la institución deberá asegurar que el resultado de la implantación de las iniciativas y proyectos de TI tenga continuidad y llegue a hacer parte de su cultura organizacional.
- h) La Dirección de TI propenderá por facilitar los trámites por parte de los diferentes grupos de interés, a partir de la implementación de herramientas tecnológicas que reduzcan gastos de tiempo y recursos innecesarios.
- i) La Dirección de TI debe proponer acciones de mejora y transformación a partir del monitoreo de la implementación de su estrategia de Uso y Apropiación y de la aplicación de mecanismos de retroalimentación.
- j) La Dirección de TI con ayuda de otras áreas es responsable de elaborar un plan de gestión del cambio para facilitar el Uso y Apropiación de los proyectos de TI. Este plan debe incluir las prácticas, procedimientos, recursos y herramientas que sean necesarias para lograr el objetivo.
- k) La Institución es responsable de asegurar el involucramiento y compromiso de los grupos de interés, en los proyectos de TI o proyectos que incorporen componentes tecnológicos partiendo desde la alta dirección hacia al resto de los niveles organizacionales.
- l) Las Unidades Administrativas y las instancias usuarias de los servicios de TI que sean convocados a las sesiones de concientización, lanzamiento y seguimiento de iniciativas de calidad, deben atender éstas oportunamente, con el fin de retroalimentar sobre el alineamiento entre la calidad gestionada por TI y los requisitos de la Institución.
- m) A través de los Servicios Web Institucionales, se cuenta con un canal de comunicación interna y externa, en donde se tiene publicada la información de interés de acuerdo con su clasificación y sus interesados.





- n) Desarrollar las competencias de TI de los directivos, funcionarios, profesores, contratistas, estudiantes, proveedores, colaboradores y visitantes, de manera que contribuyan a aumentar las capacidades de TI y la transformación requerida por la institución, a través de: charlas presenciales o virtuales, campañas de sensibilización, publicaciones, boletines informativos, cursos, apoyo de expertos y aquellas adicionales que se consideren pertinentes.

7. SEGURIDAD. Las políticas de Seguridad de la Información de la Universidad Simón Bolívar, propende por el aseguramiento de la confidencialidad, integridad, disponibilidad y privacidad de la información de la institución, es por esto por lo que se definirán todos estos requerimientos y políticas en un manual de seguridad informática que va a estar adjunto a la formulación de la Política Integral de TI. Estos se basarán en:

- a) Auditoria y trazabilidad de información
- b) Protección y privacidad de la información
- c) Seguridad y privacidad de los sistemas de información
- d) Análisis de riesgos de los sistemas e infraestructura de Información.
- e) Seguridad en Sistemas e Infraestructura tecnológica
- f) Uso de servicios tecnológicos ofrecidos por la Universidad Simón Bolívar
- g) Responsabilidades y derechos de los Directivos, funcionarios, docentes, contratistas, estudiantes, proveedores, colaboradores y visitantes de la Universidad Simón Bolívar

Responsables. Para la Universidad Simón Bolívar es fundamental tener claridad en las responsabilidades, con el fin de definir, actualizar, gestionar, dar cumplimiento y hacer seguimiento a la Política Integral de Tecnologías de la Información.

- a) **Dirección de TI.**: Es responsable del uso de la política Integral de TI como herramienta de gestión y definir los estándares para que la Universidad de cumplimiento a la misma. Poner a disposición los recursos necesarios para que las políticas de TI de la Universidad Simón Bolívar se lleven de acuerdo con los establecidos en la presente política.
Designar al personal idóneo para apoyar la implementación de la presente política. Cualquier requerimiento de modificación de las políticas debe ser dirigido a la Dirección de TI, quien será la encargada de mantener actualizada la política de TI de la Universidad Simón Bolívar.
- b) **Directivos, funcionarios, docentes, contratistas, estudiantes, proveedores, colaboradores y visitantes.**: Son responsables de dar cumplimiento a las políticas de TI
- c) **Alta Dirección:** Dará aprobación de las políticas de TI y actualizaciones de estas, previa validación de la Dirección de TI.
- d) **Coordinación de Seguridad Informática.**: Velar que el cumplimiento de la presente política se lleve a cabo de acuerdo con los lineamientos de seguridad establecidos por la Universidad Simón Bolívar.
- e) **Áreas funcionales de la Institución.**





- i. Jefaturas
 - ii. Decanaturas.
 - iii. Departamentos
- f) Coordinaciones adjuntas a la dirección de TI**
- i. Coordinación de Soporte Técnico
 - ii. Coordinación de Seguridad Informática
 - iii. Coordinación de Redes e Infraestructura Tecnológica
 - iv. Coordinación de Desarrollo de Software
 - v. Coordinación de Gestión y Analítica de datos.
 - vi. Coordinación de Proyectos TI

Artículo 9. Referencias, estándares, políticas y procesos relacionados.

1. Norma técnica NTC-ISO/IEC Colombiana 27001.
2. Nomograma de la Dirección de TI.
3. Análisis de Riesgos.
4. Procedimientos que están nombrados en los dominios
5. Compendio de la política para el desarrollo de las funciones sustantivas y administrativas de la Universidad Simón Bolívar.
6. -PED- Plan Estratégico de desarrollo de la Universidad Simón Bolívar.
7. Lista de obligaciones legales, normativas y contractuales de la universidad Simón Bolívar.
8. Marco de Referencia Arquitectura empresarial, Normatividad colombiana avalada por el MINTIC.
9. ITIL (Information Technology Infrastructure Library). Librería de Infraestructura de Tecnologías de Información.
10. Cobit: Objetivos de Control para las Tecnologías de la Información y Relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology).
11. Política de Gobierno Digital. Manual para la implementación de la estrategia de Gobierno Digital. Versión 2019.
12. TOGAF (The Open Group Architecture Framework). Marco para Arquitectura Empresarial.
13. Política de Tratamiento de datos personales de la Universidad Simón Bolívar

Artículo 10. Indicadores.

Los indicadores de esta política Integral de TI se tratarán en términos muy generales, ya que, para cada dominio, tendrá su habilitador específico dependiendo del área que se trate y se dispondrá sus métricas de medición.

Estos indicadores se basarán el principio de SMART

- específico (Specific)
- medible (Measurable)
- alcanzable (Achievable)
- orientado a resultados (Result-oriented)





- a tiempo (Timely)

Métricas

métricas	Frecuencia de medición
Cantidad de dependencias capacitadas en el año sobre la política Integral de TI	Anual
Cantidad de Incidentes de la Política Integral de TI presentadas en el año	Anual
Cantidad de Incidentes de la Política Integral de TI resueltas en el Año.	Anual
Cantidad de revisiones, actualizaciones de la Política Integral de TI gestionadas	Anual
Cantidad de Procesos de la Universidad Simón Bolívar optimizados con la Política Integral de TI	Anual

1. Porcentaje de capacitación de personal sobre Política Integral de TI

Objetivo del Indicador: Cálculo porcentual de personal de la Universidad Simón Bolívar que ha sido capacitada sobre la política de TI.

Frecuencia: Anual.

Formula:

$$\frac{\text{Cantidad de Personal Capacitado en el año sobre la Política de TI}}{\text{Cantidad de Personal vinculado a la Universidad Simón Bolívar en el año}} * 100$$

2. Índice de optimización de la Política Integral de TI a los procesos de la institución.

Objetivo del Indicador: Calcular el porcentaje de optimización de la Política Integral de TI en los procesos de la institución.

Frecuencia: Anual.

Formula:

$$\frac{\text{Numero de procesos de la Universidad Simon Bolivar}}{\text{Numero de procesos de la Universidad Optimizados con la Politica Integral de TI}} * 100$$

3. Porcentaje de Incidentes de la Política Integral de TI resueltos en el año.

Objetivo del Indicador: Calcular el porcentaje de incidentes resueltos de la Política Integral de TI

Frecuencia: Anual.

Formula:





$$\frac{\text{Cantidad de Incidentes de la Política Integral resueltas en el Año}}{\text{Cantidad de Incidentes de la política Integral presentada en el Año}} * 100$$

Artículo 11. Excepciones.

Las excepciones al cumplimiento de la Política de TI deben ser avaladas y aprobadas por la Dirección de TI de la Universidad Simón Bolívar, cuando exista alguna razón que la justifique. Todas las excepciones deben estar formalmente documentadas, registradas y revisadas por la dirección de TI. Cualquier aprobación de una excepción debe estar limitada en el tiempo y alcance.

Artículo 12. Revisiones y actualizaciones.

Las revisiones y actualizaciones de la política Integral de TI deberán estar formalmente documentadas, registradas, revisadas y aprobadas por la dirección de TI este proceso se deberá realizar anualmente para su fortalecimiento.

Artículo 13. Sanciones.

Esta política es de estricto cumplimiento y su desacato se considerará un incidente que traerá consecuencias legales; dependiendo de la gravedad, dará lugar a un proceso disciplinario contemplado en el Reglamento Interno de Trabajo y/o Reglamento Estudiantil de la Universidad Simón Bolívar.

Artículo 14. Vigencia, derogatoria y socialización.

La presente Política Integral de tecnología de la información rige a partir de su promulgación. y deroga las disposiciones que sean contrarias; permanecerá por tiempo indefinido realizando las revisiones y las mejoras según como se crea conveniente.

Cualquier cambio sustancial en la política Integral de TI, se comunicará de forma oportuna a través de los medios habituales de contacto y/o a través de áreas de comunicaciones, capacitaciones, portal web, www.unisimon.edu.co.

Una vez entre en vigencia esta política corresponde, de acuerdo con la naturaleza de la misma, proceder a su implementación, socialización y divulgación a toda la comunidad universitaria, a través de las dependencias correspondientes y acogiendo lo estipulado en la política de comunicaciones de la Institución.

Artículo 15. Cumplimiento.

La Universidad Simón Bolívar a través de la dirección de TI, velará por la identificación, documentación y cumplimiento de los requisitos enmarcados dentro de la Política a través de reportes de monitoreo, generación y uso de métricas e indicadores, auditorías y pruebas directas.





COMUNÍQUESE Y CÚMPLASE

Dado en la ciudad de Barranquilla a los diecisiete (17) días del mes de diciembre de 2020.
Para constancia firman:

JOSÉ CONSUEGRA BOLÍVAR

Rector



ROSARIO GARCÍA GONZÁLEZ

Secretaria General

FERNANDO MORÓN POLO
Director de Planeación y Responsabilidad Social