



PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN 2023



Dirección de las Tecnologías y
Sistemas de Información y
de las Comunicaciones

Dirección de las Tecnologías y Sistemas de Información y de las
Comunicaciones

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

Tabla de contenido

Tabla de contenido	2
1. INTRODUCCIÓN	3
2. JUSTIFICACIÓN	4
3. OBJETIVOS	5
3.1 OBJETIVO GENERAL	5
3.2 OBJETIVOS ESPECIFICOS	5
4. ALCANCE	6
5. NORMATIVIDAD	6
6. SITUACION ACTUAL	13
6.1 DIAGNOSTICO TRANSFORMACION DIGITAL	14
6.1.1 Panorama general	14
6.1.2 Visión y estrategia	15
<i>RECOMENDACIONES</i>	15
6.1.3 Cultura organizacional	18
<i>RECOMENDACIONES</i>	19
6.1.4 Operación	22
<i>RECOMENDACIONES</i>	22
6.1.5 Mercadeo y comunicaciones	25
<i>RECOMENDACIONES</i>	26
6.1.6 Infraestructura	29
<i>RECOMENDACIONES</i>	29
7. ESTRATEGIA DE SEGURIDAD DIGITAL	31
8. RESPONSABLES	1
9. APROBACION	1
REFERENCIAS BIBLIOGRÁFICAS	2

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

La Universidad Pedagógica y Tecnológica de Colombia con el objeto de proteger la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales como lo es el decreto 1078 de 2015 ha establecido realizar un plan de seguridad y privacidad de la información

Para la Universidad Pedagógica y Tecnológica de Colombia es de suma importancia mantener los activos de información protegidos y por ello ha implementado un adecuado conjunto de controles y procedimientos para alcanzar un correcto nivel de seguridad y de igual forma administrar y hacer seguimiento a estos controles para mantenerlos y mejorarlos a lo largo del tiempo.

El presente documento contiene el Plan de Seguridad y Privacidad de la información, orientado por un conjunto de actividades basadas en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) para crear condiciones de uso confiable en el entorno digital y físico de la información, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información.

El presente documento es el resultado de la actualización correspondiente a la vigencia 2022

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

2. JUSTIFICACIÓN

La Universidad Pedagógica y Tecnológica de Colombia reconoce que la información es uno de los activos más valiosos e importante de la organización, así mismo es indispensable para el cumplimiento de sus objetivos y de su misión, por lo tanto la información sólo tiene sentido cuando está disponible y es utilizada de forma consistente, lo cual implica que es necesario que la Universidad implemente una adecuada gestión de sus recursos y activos con el objetivo de asegurar y controlar el debido acceso, tratamiento y uso de la información.

La información puede llegar a ser sensible o crítica y por lo tanto requiere de una evaluación para determinar su nivel de protección, para mitigar o evitar posibles situaciones de riesgo.

Por lo anterior el aseguramiento y la protección de la seguridad de la información, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razón por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Establecer estrategias para garantizar la administración, manejo y control de la seguridad y privacidad de la información de la Universidad Pedagógica y Tecnológica de Colombia bajo la norma NTC/IEC ISO 27001:2013.

3.2 OBJETIVOS ESPECIFICOS

- Establecer un cronograma fundamentado en el ciclo de mejora continua para la adopción completa del MPSI.
- Implementar medidas de ejecución y de verificación de los controles previstos dentro del MPSI con base en los riesgos identificados de seguridad de la información en la universidad.
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

4. ALCANCE

El alcance del modelo de seguridad y privacidad de la información de la Universidad Pedagógica y Tecnológica de Colombia, aplica para todos los procesos, funcionarios, proveedores, contratistas, docentes y comunidad en general, que en razón del cumplimiento de sus funciones, compartan, utilicen, recolecten, procesen, intercambien o consulten información, así como a los entes de control o entidades que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación.

Apunta a proteger y preservar la integridad, confidencialidad y disponibilidad de los activos de información de la universidad

5. NORMATIVIDAD

El plan estratégico de seguridad y privacidad de la información de la Universidad Pedagógica y Tecnológica de Colombia se basa en la siguiente normatividad.

Marco Normativo	Descripción
Decreto 2150 de 1995	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 594 de 2000	Ley general de archivo
Directiva 02 de 2000	Plan de Acción de la estrategia de gobierno en línea
Directiva presidencial 10 de 2002	Programar y renovación de la administración pública: hacia un estado comunitario

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

Ley 734 de 2002	Código de Único disciplinario
CONPES 3292 de 2004	Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos.
Ley 962 de 2005	El artículo 14 lo siguiente “Cuando las entidades de la Administración Pública requieran comprobar la existencia de alguna circunstancia necesaria para la solución de un procedimiento o petición de los particulares, que obre en otra entidad pública, procederán a solicitar a la entidad el envío de dicha información. En tal caso, la carga de la prueba no corresponderá al usuario.
Decreto 1151 de 2008	Será permitido el intercambio de información entre distintas entidades oficiales, en aplicación del principio de colaboración. El envío de la información por fax o por cualquier otro medio de transmisión electrónica, proveniente de una entidad pública, prestará mérito suficiente y servirá de prueba en la actuación de que se trate, siempre y cuando se encuentre debidamente certificado digitalmente por la entidad que lo expide y haya sido solicitado por el funcionario superior de aquel a quien se atribuya el trámite”.
Ley 1273 de 2009	Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones 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
Ley 1341 de 2009	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Decreto 4485 de 2009	Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública.
Decreto 235 de 2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Norma Técnica Colombiana NTC 5854 de	Accesibilidad a páginas web El objeto de la Norma Técnica Colombiana (NTC) 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

2012	
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012" o Ley de Datos Personales.
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
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.
Ley 1753 de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAIS" "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.
Decreto reglamentario 1081 de 2015	Reglamento sobre la gestión de la información
Acuerdo 003 de 2015	Por el cual se establecen lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012"

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

Decreto 2433 de 2015	Por el cual se reglamenta el registro de TIC y se subroga el título I de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Resolución 3564 de 2015	Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones.
CONPES 3854 Política Nacional de Seguridad Digital de Colombia, del 11 de abril de 2016	El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo
Resolución 2405 de 2016	Por lo cual se adopta el modelo de sello de Gobierno Digital
Decreto 728 de 2017	Actualiza el Decreto 1078 de 2015 con la implementación de zonas de acceso público a Internet inalámbrico
Resolución 2710 de 2017	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.
Decreto 728 de 2017	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Decreto 1499 De 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Decreto 1413 de 2017	En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

CONPES 3920 de Big Data, del 17 de abril de 2018	La presente política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales.
CONPES 3975 de 2018	Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Resolución 1443 de 2018	Por el cual se sustituyen los artículos 15 y 19 y se modifica el artículo 17 de la resolución 2405 de 2016
Decreto 1008 De 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Ley 1955 de 2019	Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
Ley 1978 de 2019	Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones (TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones. Resumen de Notas de Vigencia
Decreto 2106 2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública
CONPES 3975 DE 2019	Política nacional para la Transformación Digital e Inteligencia Artificial
Circular 02 de 2019	Con el propósito de avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valor público en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad.
Directiva presidencial 02 2019	Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones
Decreto 620 de 2020	Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales
Ley 2052 de 2020	Por medio de la cual se establecen disposiciones, transversales a la rama ejecutiva del nivel nacional y territorial y a los particulares que cumplan funciones públicas y 10 administrativas, en relación con la racionalización de trámites y se dictan otras disposiciones
Resolución 1519 de	Transparencia en el acceso a la información, accesibilidad web, seguridad digital

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

2020	web y datos abiertos.
Resolución 2160 de 2020	“Por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos”
Resolución 2893 de 2020	Por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPAs y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado Colombiano, y se dictan otras disposiciones”
CONPES 3995 de 2020	Política Nacional de confianza y Seguridad digital
Directiva presidencial 03 de 2021	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”
Decreto N° 767 de 2022	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Resolución 1951 de 2022	Por la cual se establecen los requisitos, las condiciones y el trámite de la habilitación de los prestadores de servicios ciudadanos digitales especiales, se dan los lineamientos y estándares para la integración de estos servicios y la coordinación de los prestadores con la agencia nacional digital.
Decreto N° 088 de 2022	Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
Resolución 460 de 2022	Por la cual se expide el Plan Nacional de Infraestructura de datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital y se dictan los lineamientos para su implementación.
Decreto N° 338 de 2022	Por el cual se adiciona el Título 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones”
Resolución 746 de 2022	Por la cual se establece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No 500 de 2021
Resolución 1117 de 2022	Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

	marco de la Política de Gobierno Digital
Decreto N° 767 de 2022	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones'
Directiva presidencial 02 de 2022	reiteración de la política pública en materia de seguridad digital
Acuerdo 020 de 2023	Por el cual se aprueba el Plan Estratégico de Desarrollo de la Universidad Pedagógica y tecnológica de Colombia 2019 - 2030
Acuerdo de 021 de 2023	Por el cual se aprueba el Plan de Desarrollo Institucional de la Universidad Pedagógica y tecnológica de Colombia 2023 - 2026

ILUSTRACIÓN 1 *NORMATIVIDAD APLICABLE*

Fuente: *Elaboración propia*

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

6. SITUACION ACTUAL

La Universidad Pedagógica y tecnológica de Colombia ha realizado varias actividades de adopción del Modelo de Seguridad y Privacidad de la información, a continuación, se explica en cada uno de los ámbitos, cual es la situación actual de la institución

Ámbito de Seguridad y Privacidad de la Información	Situación Actual
<i>Diagnostico</i>	<p>El diagnostico se encuentra establecido en el Modelo de Seguridad y Privacidad de la información vigencia 2023-2026</p> <p>La Alta Dirección ha participado en la aprobación e implementación de Políticas de Seguridad</p> <p>La universidad cuenta con el manual de Políticas de Seguridad de la información A-RI-M03</p> <p>La Universidad cuenta con el oficial de Datos personales designado por Resolución rectoral</p>
<i>Plan de Seguridad y Privacidad de la información</i>	<p>La universidad cuenta con el documento de Declaración de Aplicabilidad A-Ri-P35-F02 la cual se encuentra debidamente diligenciada y actualizada conforme a la norma ISO 27001:2013</p> <p>Se cuenta con el Documento PSPI actualizado de forma anual</p> <p>La Universidad cuenta con el procedimiento de riesgos A-RI-P35</p> <p>La Universidad cuenta con la herramienta de identificación de activos y análisis de riesgos de seguridad</p> <p>Se cuenta con correo electrónico institucional soporte.seguridad@uptc.edu.co donde se reportan los incidentes de seguridad que se puedan presentar en la institución</p> <p>Se elaboró, publicó y socializó el procedimiento de gestión cambios A-RI-P10, que tiene por objetivo mantener la disponibilidad de los servicios de TI, frente a las solicitudes de cambio, estandarizando el registro, planeación, ejecución y monitoreo de los mismo, con el fin de reducir el impacto en la prestación del servicio.</p>
<i>Gestión de Riesgos</i>	<p>La Universidad implemento el manejo y respuesta a incidentes asociados a Seguridad y Privacidad de la Información, mediante el procedimiento denominado Gestión de Incidentes A-RI-P07.</p> <p>La Universidad, con el fin de garantizar la transferencia segura de información, requeridos por los entes de control o de otras dependencias en el marco de sus funciones, implemento la guía A-RI-P35-G01 Guía para la identificación, clasificación, gestión de riesgos y etiquetado de activos servicios y seguridad de la información.</p>

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

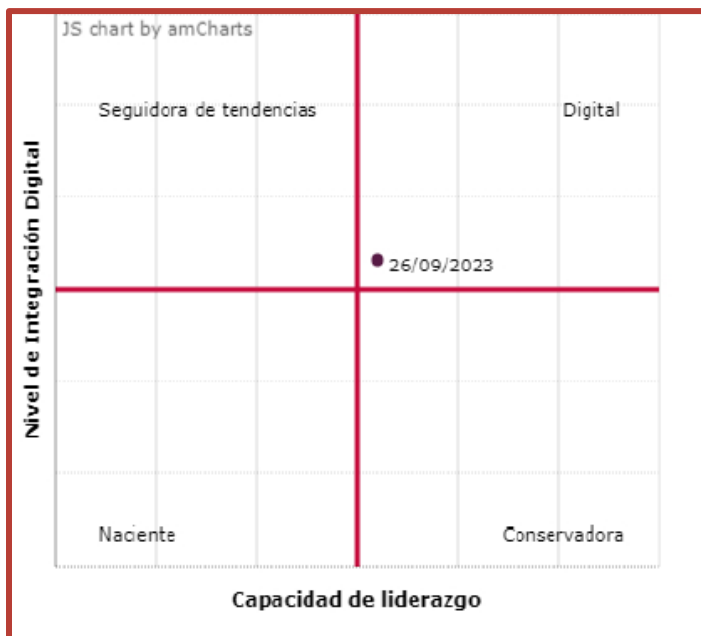
6.1 DIAGNOSTICO TRANSFORMACION DIGITAL

Se uso la herramienta NODOKA, para determinar el diagnostico o situación actual en la que se encuentra la Universidad en temas de Transformación Digital, esta herramienta arrojó los siguientes resultados:

Con el fin de garantizar la transferencia segura de datos de carácter personal requeridos por los entes de control y vigilancia en el marco de sus funciones misionales, se ha implementado el procedimiento “Intercambio Seguro de Datos con Entidades de Vigilancia y Control”.

6.1.1 Panorama general

La organización se encuentra en **ESTADO DIGITAL**



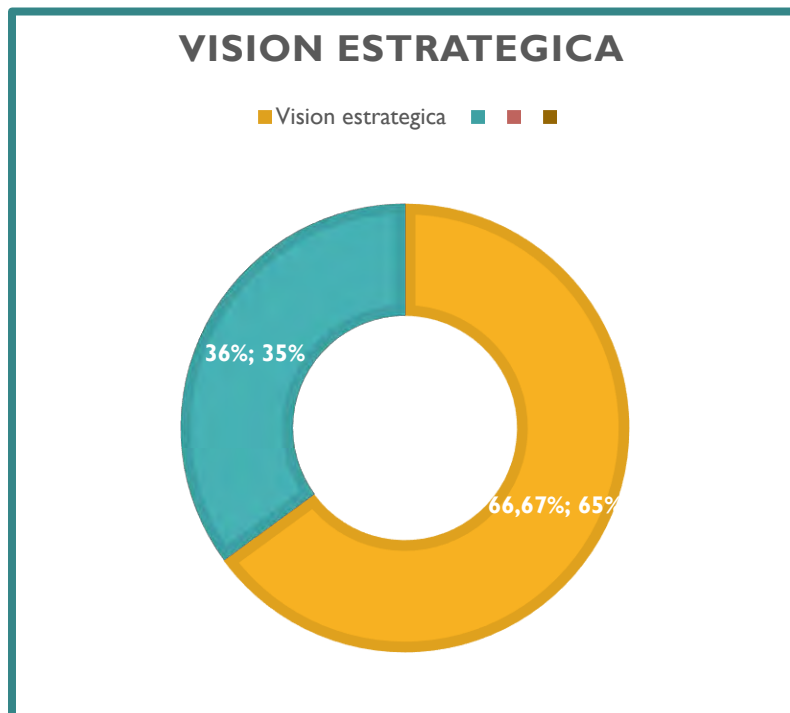
Estas empresas han analizado su visión estratégica y han reconocido que, a través del uso de la tecnología en todos los procesos, pueden maximizar sus resultados organizacionales. Aprendieron a conocer cómo generar valor a partir de la transformación digital, con una estrategia bien definida, en ejecución y evaluación continua. Han tenido la capacidad de identificar e implementar las herramientas tecnológicas que más les ayude a tener resultados de alto impacto y diferenciación

dentro de su objetivo misional. El desarrollo de una cultura digital al interior de la organización es una parte muy importante de las capacidades desarrolladas.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

El reto en este nivel es mantenerse. Contar con un modelo de medición y evaluación constante de la transformación digital, es un factor clave de éxito.

6.1.2 Visión y estrategia



La organización se encuentra en **ESTADO EXPLORADOR**

La organización ya ha empezado a incorporar el uso de la tecnología en su estrategia, cuenta con presupuesto, personal responsable y ha empezado a utilizar información sistematizada en la toma de decisiones

ILUSTRACIÓN 2 DIAGNOSTICO VISION ESTRATÉGICA

RECOMENDACIONES

- Para hacer parte de un modelo de Transformación Digital es fundamental contar con datos e información sistematizada, que permita tomar decisiones organizacionales a partir de evidencias concretas.
- Desarrolle un proceso de sistematización y/o digitalización de datos e información que permita tener información actualizada y de buena calidad.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

- Evalué herramientas digitales tales como: PowerBI, Tableau o incluso Excel, y escoja aquellas que más se adecuen a las necesidades de la organización. Considerando la importancia de contar con información actualizada en cualquier momento y lugar.
- Haga del análisis de datos e información una herramienta fundamental para la innovación y la manera como alcanza sus objetivos misionales.
- Al definir el presupuesto, tenga en cuenta todos los recursos necesarios para desarrollar la estrategia (personal, nuevos conocimientos y habilidades, diagnósticos, asesoría de expertos, etc.) no solo la incorporación de herramientas digitales.
- Es importante hacer una planeación financiera adecuada para balancear las inversiones en tecnología digital entre corto, mediano y largo plazo; también para nuevas exploraciones tecnológicas.
- Defina indicadores de medición que le permita a la organización conocer los beneficios que le genera las inversiones en Transformación Digital.
- Defina y gestione el plan de ejecución del presupuesto. Tenga en cuenta que no se tiene que ejecutar todo de una vez, sino que se pueden ir realizando acciones año a año.
- Asegúrese que sus recursos, mecanismos de financiación y visión de transformación digital estén alineados.
- Es importante empezar a concebir la incorporación de la tecnología como un elemento importante y transversal para lograr la eficiencia, eficacia y diferenciación de sus objetivos y metas. Para esto es necesario definir un direccionamiento estratégico claro y planeado

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

de la transformación digital, que esté alineado con la planeación estratégica de la organización.

- Evalúe cuales de sus estrategias organizacionales son o pueden llegar a ser valiosas en la era digital para potenciarlas.
- A partir de la visión y propósito de la organización, defina la visión digital transformadora, que tenga tanto la definición como el resultado esperado. Debe contener todas las oportunidades y retos de la organización, no solo los cambios de la tecnología. Es importante contar con una descripción más amplia, pensar que es lo que se soluciona o mejora con el uso de la tecnología.
- Para definir la estrategia de transformación digital, comience por identificar los cuellos de botella de su organización y de sus usuarios/beneficiarios y analice cuales podrían resolverse a través del uso de herramientas tecnológicas.
- Traslade la visión a acciones concretas.
- Defina indicadores de medición para monitorear la estrategia de transformación digital.
- Difunda la visión entre los miembros de la organización y permita que ellos construyan a partir de esta.
- ¡Felicitaciones! Su organización maneja un buen modelo de gobierno para la toma de decisiones de Transformación Digital.
- Empodere de manera permanente a las personas que lideran la Transformación Digital permitiéndoles ser propositivas e innovadoras.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

- Asegúrese de mantener un modelo de gobierno sólido y sostenible.
- Para lograr una ventaja y diferenciación digital se requiere liderazgo.
- Las áreas directivas deben ser conscientes de los retos digitales, y como se alinean con la visión y estrategia de la organización, entender cuál es el punto de partida y permear la visión de la TD en todas las áreas de la organización.
- Las áreas directivas deben promover el desarrollo de la Transformación digital en las organizaciones siendo los modelos para seguir en su adopción y apropiación. Deben abanderar las iniciativas de cambio y transformación digital, asegurando la alineación y empoderamiento de todas las áreas en el desarrollo de la transformación digital.
- Resalte la importancia de este tema ante el Equipo Directivo, Junta Directiva o la entidad de gobierno corporativo que corresponda en su organización, con el fin de que se incorpore como estrategia institucional.

6.1.3 Cultura organizacional

La organización se encuentra en **ESTADO BÁSICO**

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN



ILUSTRACIÓN 3 DIAGNOSTICO CULTURA ORGANIZACIONAL

Aunque los miembros de la organización cuentan con tecnologías y conocimiento, aun no se evidencia una cultura sólida donde sus miembros se apropien de ella. En muchos casos el conocimiento se da por iniciativa de las personas y no porque hace parte de una estrategia organizacional.

RECOMENDACIONES

- Para que la transformación digital tenga los resultados esperados, es importante fomentar espacios de diálogo, conexión y co-creación para dar voz a todos los miembros de la organización y permitir que surjan conversaciones, recomendaciones y/o soluciones sobre los retos y oportunidades que trae la transformación digital. Recuerde que el conocimiento y experiencia de los empleados son un activo importante para el desarrollo de una estrategia de transformación digital.
- Difunda la visión entre los miembros de la organización y permita que ellos construyan a partir de esta.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

- Ponga a prueba de manera constante su modelo de transformación digital con el equipo de trabajo, para encontrar oportunidades de mejora.
- La transformación digital se logra elevando el coeficiente intelectual digital de los miembros de la organización; comience construyendo las habilidades digitales adecuadas.
- Realice un análisis de las habilidades digitales de cada una de las personas, así como un plan de formación según su cargo. Es importante definir planes de formación continuos y actualizados, liderados por la organización, para la apropiación de tecnologías digitales que permitan un mejor desempeño de las funciones y el cumplimiento de los resultados organizacionales.
- Puede fomentar el uso de cursos gratuitos disponibles en plataformas como: <https://www.coursera.org/> , <https://www.edx.org/es> , <https://miriadax.net/home> o <https://learndigital.withgoogle.com/garagedigital>
- Para el desarrollo de la transformación digital en las organizaciones, es fundamental garantizar que los miembros de la organización tengan acceso, conocimiento y uso recurrente de herramientas digitales.
- Desarrolle estrategias para motivar a sus equipos en la utilización de la tecnología para el mejoramiento y optimización de su labor y para transformar la manera como ejecutan sus funciones, buscando mayor eficacia y mejores resultados.
- Es importante crear modelos de aprendizaje y mejoramientos continuo de habilidades y herramientas digitales al interior de la organización.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

- Utilice la tecnología digital como medio para involucrar y empoderar a los empleados en la estrategia de la organización.
- Las organizaciones deben asumir el reto del cambio permanente para lograr la sostenibilidad.
- Nuevos descubrimientos reemplazan rápidamente la manera como estamos acostumbrados a hacer las cosas, por lo tanto, es indispensable desarrollar modelos de gestión del cambio dentro de las organizaciones que permitan a todos estar preparados para asumir la transformación digital.
- La transformación digital necesita personas abiertas al cambio, por lo que es importante desarrollar estrategias que promuevan la flexibilidad de pensamiento, la apertura a nuevas maneras de hacer las cosas, de adaptarnos y apropiarnos de los cambios, descubriendo las oportunidades y beneficios que estos traen para las personas y la organización. Estas estrategias deben estar dirigidas a todos los miembros de la organización.
- Un elemento importante que genera sensibilización y consciencia sobre la transformación digital, es comunicar las victorias tempranas que se vayan implementando con los resultados y beneficios que esto genera en el cumplimiento de los objetivos propuestos.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

6.1.4 Operación

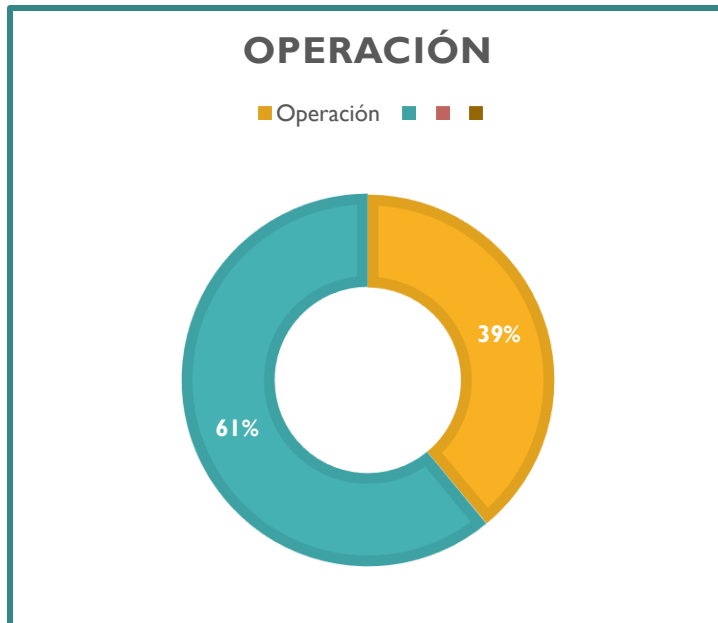


ILUSTRACIÓN 4 DIAGNOSTICO OPERACIÓN

La organización se encuentra en **ESTADO BÁSICO**

La organización utiliza herramientas de tecnología para el desarrollo de algunos procesos internos y de proyectos, pero no se ha atrevido a utilizarla como herramienta de diferenciación para alcanzar sus objetivos. Existen políticas poco seguras para el almacenamiento de la información

RECOMENDACIONES

- La información es uno de los activos más importantes de una organización social y como tal, se debe proteger, no solo de la posible pérdida o daño de un dispositivo (computador o servidor) sino de la fuga de propiedad intelectual.
- Lo ideal es llegar a tener toda la información en la nube, centralizada, organizada y con los adecuados niveles de acceso según los cargos y responsabilidades de las personas. Inicie analizando sus procesos y requerimientos de información, y con base en esto diseñe una política de gestión documental y una taxonomía de contenidos. Este proceso debe ser colaborativo. Posteriormente, inicie un proceso de migración de información a la nube.
- En <http://techsoup.global> puede encontrar de manera gratuita o a bajo costo, herramientas

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

de almacenamiento en la nube como: Box, SharePoint y OneDrive de Office365 y GoogleDrive de G-Suite.

- La incorporación de la transformación digital a la gestión de proyectos permite lograr mayor eficiencia y eficacia en la toma de decisiones, siendo a la vez una herramienta potente de mitigación de riesgos para la gestión de los resultados y el cumplimiento de los objetivos.
- Evalué los cuellos de botella e ineficiencias de los procesos de gestión de proyectos e identifiqué si las tecnologías digitales existentes pueden ayudarle a mejorar sus resultados.
- Considere si es momento de reemplazar herramientas actuales por nuevas versiones tecnológicas, si los actuales no generan los resultados esperados.
- En <https://techsoup.global/> puede adquirir de manera gratuita o altamente descontada herramientas para la gestión de proyectos como Project, Excel, Planner de Office365, Teams de Office365 y muchos más.
- En <https://www.edx.org/es/course/gestion-de-proyectos-de-desarrollo-1> puede tomar un curso de Gestión de Proyectos 100% gratuito.
- La transformación digital permite a las organizaciones diferenciar su propuesta de valor e innovar ya sea en la oferta de productos o servicios o en la manera como se entrega la experiencia al usuario/beneficiario. Es importante crear espacios de ideación para encontrar elementos que permitan hacer las cosas distintas a como lo hace el sector social en general, por medio de la transformación digital. Escuchar la voz del usuario/beneficiario, es un factor fundamental para identificar oportunidades de innovación.
- Considere transformar su nivel de impacto social conectando sus productos, servicios e

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

información con herramientas innovadoras que le permitan crear más valor.

- La incorporación de la transformación digital en los procesos administrativos y de soporte organizacional permite lograr mayores eficiencias y mejorar los resultados. Evalúe los cuellos de botella e ineficiencias de los procesos internos y considere si las nuevas tecnologías digitales existentes pueden ayudarle a mejorar sus resultados.
- Considere si es momento de reemplazar herramientas actuales por nuevas versiones o tecnologías, si los actuales no generan los resultados esperados.
- Herramientas contables en la nube como Alegra tienen versión gratuita para organizaciones sociales: <https://www.alegra.com/> fundaciones
- Tenga en cuenta que en <https://techsoup.global/> puede adquirir de manera gratuita o altamente descontadas herramientas de análisis de gestión documental y, manejo de procesos Gsuite de Google y Office365 de Microsoft.
- La movilidad, es decir la capacidad de trabajar desde cualquier lugar, es fundamental en todas las funciones de una organización no solo para ser más eficiente sino para aquellos casos donde el teletrabajo es una opción. Esto le permite a las personas, desde donde estén, trabajar y tener acceso a la información que necesiten, sin importar el dispositivo que utilicen.
- Si algunos empleados ya tienen movilidad, verifique qué procesos o información son los más apropiados para continuar con la estrategia de movilidad. Recuerda que esto requiere un cambio cultural.
- En <http://techsoup.global> puede encontrar de manera gratuita o a bajo costo, herramientas

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

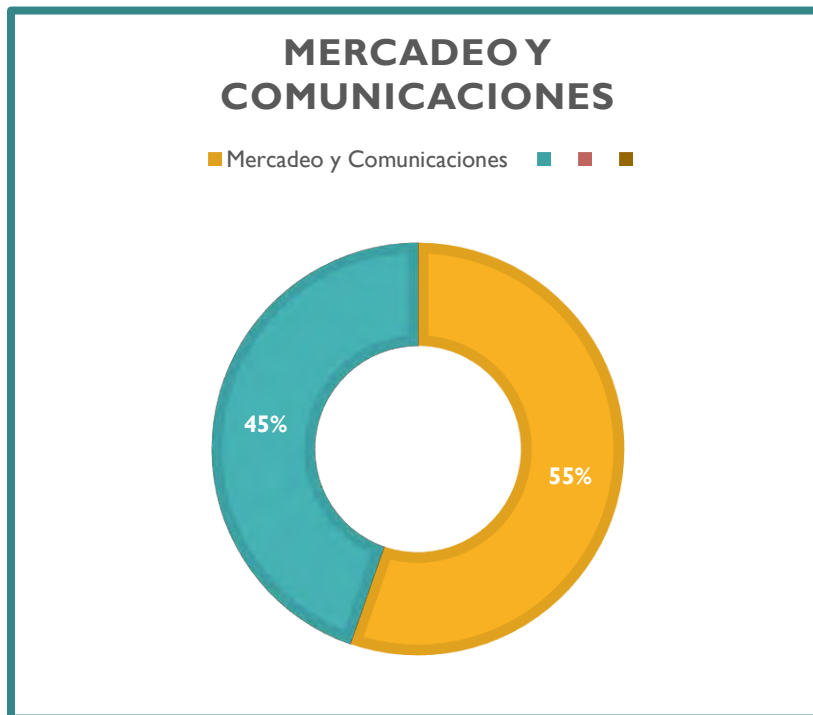
que le permiten facilitar el correo electrónico, calendario, archivos, mensajería instantánea a todos los empleados, para que tengan acceso a la información en cualquier momento. Los mejores ejemplos son Office365 y GSuite.

- Conocer las necesidades de los usuarios/ beneficiarios es proceso fundamental para desarrollar ofertas de valor diferenciadas e innovadoras. Es importante desarrollar estrategias adecuadas para escuchar a los usuarios/beneficiarios usando herramientas tecnológicas que hagan más fácil y eficiente el proceso.
- Existen varias herramientas que permiten innovar en la forma en la que se recoge información de los beneficiarios, por ejemplo:
 - Encuestas: Formularios de Office365 y de G-Suite y SurveyMonkey
 - Kahoot: para encuestas dinámicas y divertidas en tiempo real, usando celulares
 - WorldCould: para recoger información en tiempo real y ver tendencias.
 - En <http://Techsoup.global> puede acceder a Forms (Office365 y G-Suite) de manera 100% gratuita.

6.1.5 Mercadeo y comunicaciones

La organización se encuentra en **ESTADO EXPLORADOR**

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN



La organización utiliza herramientas tecnológicas para comunicarse con la mayoría de sus grupos de interés y para desarrollar estrategias de gestión de cooperantes y recursos, pero no lo hace de manera frecuente. Cuenta con una estrategia de mercadeo digital, pero se ejecuta de manera incipiente

ILUSTRACIÓN 5 DIAGNOSTICO MERCADEO Y COMUNICACIONES

RECOMENDACIONES

- La realidad de las organizaciones sociales hoy en día es que debemos tener múltiples fuentes de recursos. Una de las fuentes es la cooperación nacional e internacional y otra son las donaciones de personas (donantes individuales). Aunque depende de la estrategia de cada organización, cada vez se hace más necesario tener una comunicación constante con aliados, cooperantes y pares, no solo para buscar recursos sino para intercambiar conocimiento.
- No se trata de tener herramientas solo por tenerlas. Analice cuales y cuantas tiene la capacidad de manejar y está alineadas con su estrategia. GlobalGiving es una plataforma para recibir donaciones en línea de personas, Benevity (a través de techsoup.global) es para recibir donaciones de empresas, y www.nodoka.co es una plataforma de MAKAI para encontrar cooperantes y fondos.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

- En una realidad digital como la que vivimos hoy, te recomendamos tener como mínimo una cuenta de Facebook que te permita tener una comunidad de personas y organizaciones de tu público de interés, con el fin de generar contenidos que agreguen valor para ellos.
- Es recomendable tener un sitio web que le permita darse a conocer en los motores de búsqueda de internet, con el fin de que seas fácilmente encontrado y referenciado en internet.
- Así mismo, desarrollar parrillas de contenido, te permitirá empezar a generar información para los diferentes canales (redes sociales, website) que agreguen actividades de mercadeo digital. Aquí encontrarás algunas plantillas que te ayudarán en la estructuración: <https://materiales.rdstation.com/planilla-editable-gestion-contenido>
- Actualmente existen herramientas que permiten que el sitio web no solo sea un medio de comunicación, sino que permiten también medir tráfico y estadísticas de ingresos. Esta es una herramienta muy importante para tomar decisiones de comunicación alineadas con la estrategia. Recomendamos utilizar herramientas como GoogleAnalytics, Matomo y OpenWeb Analytics que permiten medir el tráfico del sitio web.
- En techsoup.global puede obtener 10,000 dólares mensuales de publicidad gratuita en Google a través de GoogleAds. Esto le ayudará a aumentar el tráfico a su sitio web.
- Entrar en la era de la transformación digital requiere implementar nuevas maneras de relación con los públicos para entender sus necesidades y proporcionarles una mejor propuesta de valor.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

- Considere si es momento de reemplazar herramientas actuales por nuevas versiones o tecnologías, que permitan llevar a cabo un mejor relacionamiento
- Puede utilizar herramientas como MailChimp para el envío de boletines digitales o WhatsApp para negocios para facilitar comunicación con personas. En cualquier caso, recuerde cumplir con la legislación local de uso de datos de las personas.
- También puede utilizar Teams, Hangout o Zoom para realizar videoconferencias. Todas estas herramientas disponibles en <http://techsoup.global>
- ¡Felicitaciones! Continúe aumentando el alcance y la participación de sus grupos de interés a través de nuevos canales digitales.
- No se trata de tener redes sociales solo por tenerlas. Es mejor tener pocas, o una sola, pero actualizadas y que sean las que permiten una mejor comunicación con los grupos de interés.
- Asigne una persona responsable de este tema alineado con la estrategia de comunicaciones.
- Para facilitar la gestión de mensajes y de redes, puede utilizar herramientas como hootsuite, onlypult.com y text overlay entre otros que le permiten gestionar mensajes, asignarles fechas de publicación, entre otros.
- Para diseñar imágenes atractivas, en techsoup.global puede acceder a bajo costo a herramientas como Adobe Creative Cloud y Zoner.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

- ¡Felicitaciones! Es importante mantener políticas de seguridad de información y uso de datos actualizada y que todos los miembros de la organización la conozcan y adapten.
- Si hoy en día estas pagando por los correos, te puedes ahorrar estos recursos. Accede a techsoup.global y aplica para recibir la donación de Office365 o de G-Suite a través de las cuales puedes crear correos electrónicos institucionales, de manera ilimitada . Recuerda que antes, debes tener un dominio .ORG el cual puedes registrar en www.godaddy.com.

6.1.6 Infraestructura

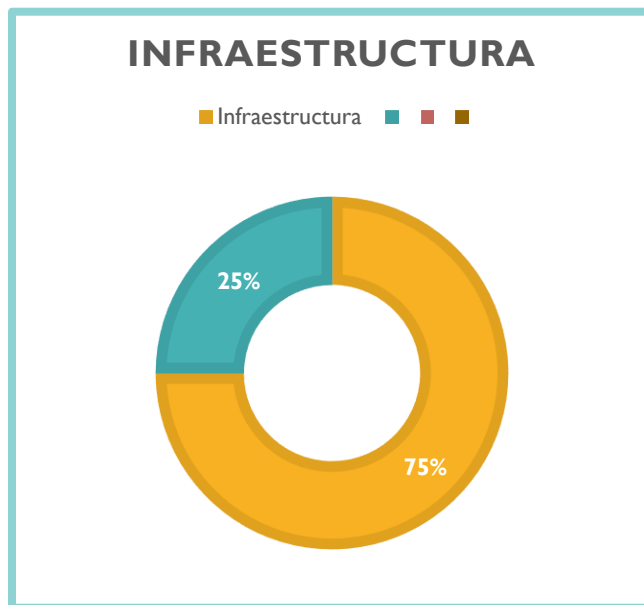


ILUSTRACIÓN 6 DIAGNOSTICO INFRAESTRUCTURA

La organización se encuentra en **ESTADO EXPLORADOR**

La organización cuenta con políticas de seguridad informática medianamente seguras, la renovación tecnológica se hace con frecuencia y su conectividad es buena y permanente, pero no está disponible a todos los miembros de la organización.

RECOMENDACIONES

- ¡Felicitaciones! Siga realizando un correcto seguimiento a las actualizaciones de su software, verifique periódicamente que sus licencias cuenten con la descarga de actualizaciones que mejoren su gestión y al ir adquiriendo nuevos equipos que éstos

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

cuenten con las licencias correspondientes al uso que les va a dar, así mismo que cuenten con seguro de software lo que le dará tranquilidad en este tema.

- Puede hacer uso del programa de donaciones de software de TechSoup en <https://techsoup.global/> para tener las mejores licencias comerciales a precio descontado.
- También puede utilizar programas de Código Abierto (Open Source) como OpenOffice.
- Felicidades, con una buena conectividad garantizas un proceso más efectivo con tu equipo de trabajo, recuerda mantener el Ancho de banda mínimo por empleado, incrementando en los casos que sea necesario el ancho de banda conforme tu equipo de trabajo crezca.
- Te recomendamos aprovechar la buena conectividad que tienes implementando servicios en la nube que te permitan potenciar tu organización.
- Se recomienda contar con un equipo técnico especializado (interno o externo) que pueda brindar soporte y manejo al firewall de la organización.
- Se recomienda adquirir software licenciado antimalware, antivirus, instalar un firewall y demás programas que prevengan de ataques a la red de la organización. En <http://techsoup.global> puede tener acceso a antivirus y plataformas de seguridad a precios especiales.
- Se recomienda tener un sistema de gestión documental definido y claro para evitar multiplicar software malicioso en transferencia de archivos. En <http://techsoup.global> puede tener acceso gratuito a Office365 y GSuite.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

- Se recomienda congelar los equipos de cómputo para evitar la instalación de software que no esté regulado y que haya sido descargado de manera sospechosa.
- Se recomienda un plan de capacitación sobre la reglamentación vigente en cuestiones de seguridad y delitos informáticos.
- Se recomienda mantener los equipos actualizados.
- Realice un diagnóstico listando de manera detallada cada uno de los equipos, su licenciamiento y su estado.
- Realice un plan de mantenimiento correctivo para todos los equipos con el fin de aumentar su vida útil. Sabemos que esto implica costos, pero es importante hacerlo. Piense en esto como una inversión. Revise también si es más costoso reparar un equipo o estarlo reparando, que comprar uno nuevo.
- Al menos cada año, vuelve a revisar el estado de los equipos y determinar cuáles deben ser reemplazados.

7. ESTRATEGIA DE SEGURIDAD DIGITAL

La Universidad Pedagógica y Tecnológica de Colombia define, implementa, evalúa y mejora las estrategias de seguridad digital en la que se integran los principios, políticas, procedimientos, manuales y lineamientos para la gestión de la seguridad de la información con base en el Modelo de Seguridad y Privacidad de la Información, así como en la política de riesgos de la Universidad

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

Con respecto a lo descrito anteriormente la Universidad Pedagógica y Tecnológica de Colombia define las 5 estrategias específicas que permitirán establecer una estrategia general con respecto a la Seguridad Digital que se muestran a continuación.



ILUSTRACIÓN 7 ETAPAS DE LA ESTRATEGIA DE SEGURIDAD DIGITAL

7.1 DESCRIPCIÓN DE LAS ESTRATEGIAS

A continuación, se describen cada una de las estrategias específicas a implementar descritas en la resolución 500 de 2021.

7.1.1 LIDERAZGO DE SEGURIDAD DE LA INFORMACIÓN

El director de las Tecnologías y Sistemas de Información es el líder del proceso de Gestión y recursos informáticos con autoridad suficiente y responsable de rendir cuentas de la eficacia del

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

SGS y SGSI ante la universidad, de acuerdo al plan de Gestión de servicios y Seguridad de la Información que soporte las políticas, los objetivos y definir las pautas para el cumplimiento de los requisitos.

7.1.2 GESTIÓN DE RIESGOS

La gestión de los riesgos se administrará según la guía metodológica de gestión de riesgos determinada por el Departamento administrativo de la función pública, en la cual se establecen los métodos para gestionar los riesgos de tal manera que las partes interesadas sean respetadas y se dé cumplimiento a los requisitos

7.1.3 IMPLEMENTACIÓN DE CONTROLES

Se deben implementar los controles seleccionados a través de la ejecución de los proyectos de seguridad definidos, estos están verificados por el Líder del SGSI. por medio del análisis de las mediciones de la eficacia de dichos controles mediante la guía A-RI-P35-G01 GUIA IDENTIFICACIÓN, CLASIFICACIÓN, GESTIÓN DE RIESGOS Y ETIQUETADO DE ACTIVOS, SERVICIOS Y SEGURIDAD DE LA INFORMACIÓN, ya que esto permite a la Universidad y al personal responsable de dichos controles determinar la medida en que se cumplen los objetivos de control seleccionados. Lo anterior, debe desarrollarse mediante la actividad de medición de la efectividad de los controles diligenciando el formato A-RI-P35-F01 IDENTIFICACIÓN, CLASIFICACIÓN, GESTIÓN DE RIESGOS Y ETIQUETADO DE ACTIVOS, SERVICIOS Y SEGURIDAD DE LA INFORMACIÓN del SGS Y SGSI.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

7.1.4 GESTIÓN DE INCIDENTES

Las incidencias de seguridad de la información se direccionan de acuerdo a su prioridad, donde La Dirección de la Tecnologías y Sistemas de la información y de las Comunicaciones es la responsable de resolver estos incidentes de acuerdo al procedimiento de Identificación, Clasificación y Gestión de Riesgos de Activos de Información y etiquetado de la información (A-RI-P35), además es la encargada de mantener informado a los procesos sobre las acciones o amenazas que atenten contra la seguridad de la información.

7.1.5 CONCIENTIZACIÓN

La Dirección de Tecnologías y Sistemas de Información y de las Comunicaciones vela por el cumplimiento de las políticas del SGSI y del SGS y las políticas del Manual de Políticas de Seguridad de la información, socializándolas tanto al interior del equipo de trabajo como a la comunidad universitaria en general y realiza su autoevaluación con un conjunto de elementos de control que permiten medir la efectividad y los resultados de la gestión, así como de la comunicación de los ejes del Plan de Desarrollo Institucional y la toma de conciencia de la eficacia del SGSI y del SGS, verificando su capacidad para cumplir las metas, los resultados y tomar las medidas que sean necesarias al cumplimiento de los objetivos previstos por la entidad.

8.2 PORTAFOLIO DE PROYECTOS (PLAN DE DESARROLLO 2023-2026)

Eje	Área	Descripción	Entregable	Hoja de Ruta													
				E	F	M	A	M	J	J	A	S	O	N	D		
Transformación Digital	Transformación de la Información	Identificar los riesgos de información e implementar políticas y controles para minimizar la materialización de estos	Matriz de identificación de activos y análisis de riesgos debidamente diligenciada						X								
	Seguridad de los Servicios ciudadanos digitales	Revisar políticas y documentación relacionada con la protección de datos personales	Divulgar la guía A-RI-P35-G01 con el fin de que toda la Universidad conozca los parámetros que se deben tener en cuenta para la transferencia de información relacionada con datos personales														
Riesgos	Matriz de identificación de activos y análisis de riesgos	Realizar actualización de la matriz de identificación de activos y análisis de riesgos	matriz de identificación de activos y análisis de riesgos publicada														
Sensibilización	actualización del plan de sensibilización y comunicaciones de la DTIC	Realizar la actualización y verificación del Plan de Comunicaciones	Plan de Comunicaciones														
		Realizar sesiones de sensibilización sobre seguridad de la información y controles del sistema de gestión de seguridad de la información institucional.	Implementación del Plan de Seguridad y privacidad de la información														
Ciberseguridad	Reinducción e inducción de funcionarios (apoyo a GGH)	Apoyar las actividades de inducción y reinducción de los funcionarios de la entidad con charlas en materia de seguridad de la información, protección de datos personales y controles el sistema de gestión de seguridad de la información															
	Seguridad en el puesto de trabajo	Apoyar técnicamente la implementación de soluciones de seguridad que protejan las estaciones de trabajo institucionales frente a software malicioso o fuga de información	Tips de seguridad														

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

Continuidad del negocio	Controles de seguridad de la información	Apoyar técnicamente el diseño e implementación de controles de seguridad que aprovechen las soluciones colaborativas y de ofimática disponibles en la Entidad	Controles de seguridad de la información																		
	Plan de Continuidad	Diseñar y desarrollar el Plan de continuidad de la universidad	Plan de Continuidad																		
		Desarrollar implementación del Plan de Continuidad de Negocio Institucional																			
		Revisar y hacer la evaluación de la implementación del plan de continuidad	Evaluación del Plan Continuidad																		

8. RESPONSABLES

La Universidad Pedagógica y Tecnológica de Colombia debe establecer un equipo de Seguridad de la Información conformada de la siguiente manera:

ASIGNACION DE ROLES, RESPONSABILIDADES Y AUTORIDADES		
ROL	CARGO	RESPONSABILIDAD
<i>Alta dirección</i>	Rector	Este equipo será responsable de apoyar a RSI en la implementación y mantenimiento del SGSI, así como en la identificación y gestión de los riesgos de la información.
<i>Delegado de la alta dirección ante las normas ISO 20001 e ISO 27001</i>	Director de Tecnologías y sistemas de información y de las comunicaciones	
<i>Equipo de gestión de DTIC</i>	Equipo de trabajo de la Dirección de Tecnologías de la Información y de las comunicaciones	
<i>Desarrolladores DTIC</i>		
<i>Gestor DBA</i>	Líder de procesos de Gestión de la contratación (acuerdo N° 001 de 2018)	
<i>Soporte a SI</i>		
<i>Equipo de infraestructura</i>	Líder de procesos de gestión de talento humano	
<i>Oficial de datos personales</i>		
<i>Encargado de gestionar los acuerdos de confidencialidad y manual de políticas de seguridad de la información con los proveedores con contratistas.</i>		
<i>Encargado de gestionar los acuerdos de confidencialidad con los funcionarios</i>		

http://www.uptc.edu.co/export/sites/default/secretaria_general/rectoria/resoluciones_2023/Resolucion_4529_2023.PDF

9. APROBACION

El presente Plan de Seguridad y Privacidad de la Información ha sido sometido a consideración y conocimiento del representante a la alta dirección de las normas ISO 20001:2018 e ISO 27000-1:2023, con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

REFERENCIAS BIBLIOGRÁFICAS

DOCUMENTOS INTERNOS

Manual del Sistema de Gestión y Seguridad de la Información

DOCUMENTOS EXTERNOS.

- Directrices y Guía emitida por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC.
- Modelo de Seguridad y Privacidad de la información v3.0.2.
- Decreto 612 de 2018 – Integración Planes Institucionales, Función Pública
- Decreto 1008 de 2018 – Política de Gobierno Digital y Manual respectivo.
- Norma ISO 27001:2013.
- Resolución 1581 de 2012 y Decreto Reglamentario 1377 de 2013 – Protección de Datos Personales.
- Resolución 500 de 2021. “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.
- Directrices emitidas por la Superintendencia de Industria y Comercio – SIC en materia de Datos Personales.
- Buenas prácticas y normatividad vigente sobre la materia.
- Ley 44 de 2093. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- 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 y se dictan otras disposiciones.