PLAN DE COMUNICACIÓN Y SENSIBILIZACIÓN 2026

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

TABLA DE CONTENIDO

INTRODUCCIÓN 3
1. OBJETIVOS 4
1.1 General 4
1.2 Específicos 5
2. ALCANCE 5
3. ROLES Y RESPONSABILIDADES 5
4. FASES DEL PLAN 6
4.1 Fase de Diseño 8
4.1.1 Identificación de necesidades 8
4.1.2 FASE DE DESARROLLO 10
4.1.3 FASE DE IMPLEMENTACION 28
4.1.3.1 Socialización del plan con la alta dirección 28
4.1.4 Técnicas recomendadas para comunicación de información 28
4.1.5 FASE DE MEJORAMIENTO 31
Objetivos de la Mejora 32
Glosario 33

INTRODUCCIÓN

e los servicios de TI y la protección integral de los activos de información son pilares estratégicos para garantizar la continuidad, calidad y transparencia de las operaciones en la Universidad Pedagógica y Tecnológica de Colombia (UPTC). Para materializar este propósito, la institución ha consolidado la adopción de los estándares internacionales ISO/IEC 20000-1:2018, que establece el Sistema de Gestión de Servicios (SGS), e ISO/IEC 27001:2022, que proporciona el marco de acción para el Sistema de Gestión de Seguridad de la Información (SGSI). Esta integración normativa asegura la entrega de servicios tecnológicos alineados con las necesidades de la comunidad universitaria, al tiempo que salvaguarda la confidencialidad, integridad y disponibilidad de la información frente a los riesgos y amenazas del entorno digital.

El presente Plan de Comunicaciones tiene como objetivo principal estructurar, optimizar y articular la difusión de información relacionada con la planificación, implementación, mantenimiento y mejora continua de ambos sistemas de gestión en la DTIC. A través de estrategias de comunicación asertivas y focalizadas, se busca sensibilizar a directivos, administrativos, docentes y estudiantes sobre su rol activo y responsabilidad en la protección de los datos y el uso adecuado de la infraestructura tecnológica. Esta sinergia es vital para consolidar una auténtica cultura de seguridad de la información y excelencia operativa al interior de la universidad.

Con un enfoque preventivo y basado en el cumplimiento normativo aplicable (incluyendo la Ley 1581 de 2012 y el Modelo de Seguridad y Privacidad de la Información del MinTIC), este documento define con precisión las audiencias objetivo, los mensajes clave y los canales oficiales de transmisión. De esta manera, se garantiza que la información fluya de manera clara, oportuna y medible. Con la ejecución de este plan, la UPTC reafirma su compromiso con el Gobierno de TI, el aseguramiento de sus procesos y el aporte de valor tecnológico para el desarrollo académico y administrativo de nuestra institución

1. VERSIONAMIENTO

Revisión	Fecha	Comentarios	Realizado Por
1	15/2/2019	Versión Inicial	Equipo de Gestión y Gobierno de TI
2	11/2/2020	Cambios anuales del plan de	Equipo de Gestión y Gobierno de TI
3	14/2/2021	Cambios anuales del plan de	Equipo de Gestión y Gobierno de TI
4	20/2/2022	Cambios anuales del plan de	Equipo de Gestión y Gobierno de TI
5	25/2/2023	Cambios anuales del plan de	Equipo de Gestión y Gobierno de TI
6	10/2/2024	Cambios anuales del plan de	Equipo de Gestión y Gobierno de TI
7	9/4/2025	Cambios anuales del plan de	Equipo de Gestión y Gobierno de TI
8	20/5/2026	Cambios anuales del plan de comunicaciones	Equipo de Gestión y Gobierno de TI

2. OBJETIVOS

2.1 General

Desarrollar e implementar un plan integral de comunicaciones y sensibilización en la Dirección de las Tecnologías de la UPTC, alineado a los principios y objetivos del marco de Gobierno Digital, con el propósito de fortalecer la adopción efectiva de nuevas tecnologías de la información y comunicación, promoviendo la conciencia digital, y optimizando la eficiencia y transparencia en los procesos institucionales, contribuyendo así al avance y consolidación de la transformación digital en la universidad.

2.2 Específicos

Asegurar que todos los aspectos de la gestión de servicios de TI, la gestión de la seguridad de la información y el cumplimiento normativo se comuniquen de manera clara y accesible para todos los niveles de la comunidad universitaria.

Fomentar la retroalimentación a través de los canales de comunicación para mejorar continuamente los procesos y servicios de TI, alineándose con los principios de mejora continua de la norma ISO 20000-1 y la evaluación de riesgos de la ISO 27001.

Sensibilizar a la comunidad universitaria sobre la importancia de la transformación digital y el papel fundamental de las TIC en la mejora de los procesos académicos y administrativos.

3. ALCANCE

Concientizar a los miembros de la comunidad universitaria para que puedan comprender y aplicar los principios de gestión de servicios de TI y seguridad de la información, conforme a las normas ISO 20000-1:2018 e ISO 27001:2022. A través de una comunicación eficaz, accesible y continua, se buscará no solo el cumplimiento de los estándares, sino también el fomento de una cultura de seguridad y mejora continua dentro de la universidad.

4. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades designados por parte del representante ante la alta dirección en las normas ISO 20001:2018 e ISO27001:2022 se encuentran publicados en el Mapa de procesos, proceso de gestión de recursos informáticos Plan de Gestión de servicios de TI y seguridad de la Información A-RI-L03, adicionalmente en la resolución 1372 del 2023 se designa a un funcionario como oficial de protección de datos, en la resolución 4686 del 2023 se designa a un funcionario como gestor de Gobierno Digital y en la resolución 1314 del 2024 se designa a un oficial de seguridad y privacidad de la información.

5. FASES DEL PLAN

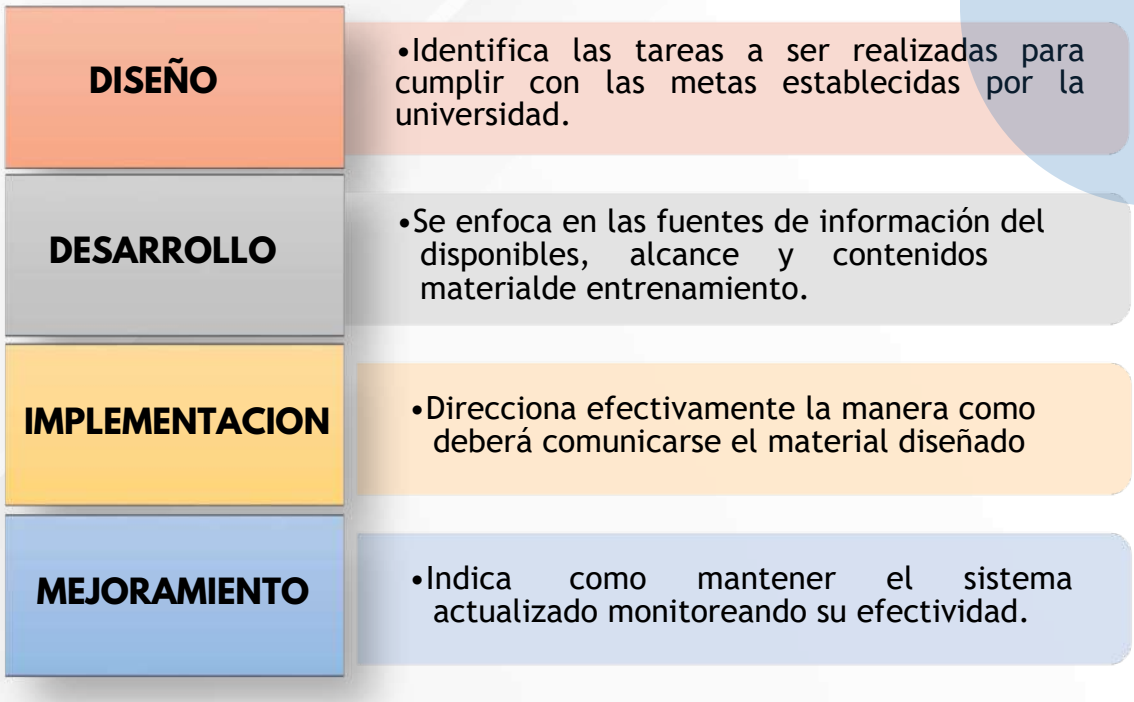


Ilustración 1 Fases plan de sensibilización, capacitación y comunicación

Fuente: Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información, MINTIC 2016

Previo a la identificación de cada una de las fases, es conveniente definir y diferenciar los siguientes términos: SENSIBILIZACIÓN, ENTRENAMIENTO, EDUCACIÓN y DESARROLLO PROFESIONAL ya que cada uno de ellos tiene un fin particular dentro del plan y dentro de la Entidad.

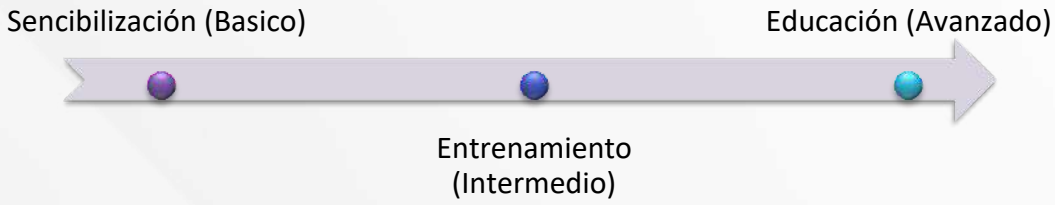


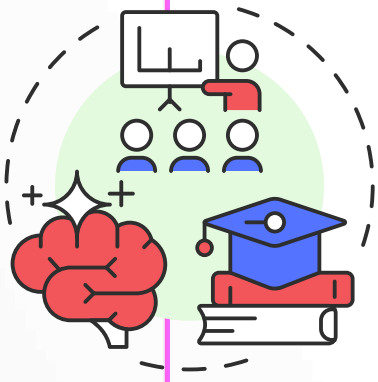
Ilustración 2 Relación entre sensibilización, entrenamiento y educación

SENSIBILIZACIÓN: Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

EJEMPLO: Uso correcto de contraseñas, consecuencias reales sobre prestar una contraseña y qué hacer si no recuerdo mi contraseña. El éxito de la sensibilización es la practicidad y la simplicidad en que esta información es entregada, para captar la atención del aprendiz.

ENTRENAMIENTO: Busca enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo. Un programa de entrenamiento no busca certificar (aunque puede llegar a hacerlo), pero puede tener mucha temática relacionada con un curso de certificación.

EJEMPLO: Un curso de seguridad de la información, enfocado a administración de riesgos, ciclo de vida del servicio de seguridad y controles operacionales.



EDUCACIÓN FORMAL: Se define como todos los niveles y habilidades de seguridad envueltos en un único cuerpo de conocimiento.

EJEMPLO: Programa de estudios de educación superior, postgrados, etc…

5.1 Fase de Diseño

La fase de diseño del plan de capacitación y sensibilización de la Dirección de las Tecnologías y Sistema de Información y de las comunicaciones (DTIC) de la UPTC, es decisivo para garantizar su efectividad y alineación con los objetivos planteados.

5.1.1 Identificación de necesidades

Para llevar a cabo esta fase se realizará un análisis de las necesidades para identificar las áreas de capacitación requeridas por la UPTC, para lo cual realizaremos varias estrategias que nos llevaran a obtener los resultados esperados.

A continuación, se describirán cada una de las actividades que se realizarán dentro de la fase de identificación de necesidades para las cuales nuestros participantes será la comunidad universitaria (Estudiantes, docentes, administrativos etc.).

Dentro de las estrategias identificadas a realizar se encuentran enmarcadas las siguientes:

ACTIVIDAD 1: REALIZAR ENCUESTA COMUNIDAD UNIVERSITARIA
"Tecnologías de la Información (TI) en la UPTC."

Esta actividad se realizará con el fin de conocer las necesidades de capacitación en el área de Tecnologías de la Información (TI) para poder ofrecer a futuro programas o instrumentos formativos que se ajusten a los requerimientos y expectativas de la comunidad universitaria.

Mediante la realización de esta encuesta se pretende conocer las opiniones de la comunidad universitaria en cuanto al nivel de conocimiento que tienen sobre Tecnologías de la Información y si consideran importante tener conocimientos en esta área, de igual forma se pretende conocer las preferencias de aprendizaje para de esta manera lograr impartir la información de una forma agradable.

ACTIVIDAD 2: SENSIBILIZAR A LA COMUNIDAD UNIVERSITARIA

La sensibilización continúa en Seguridad de la Información dentro de la UPTC es esencial para mantener en alerta a toda la comunidad y comprometidos con las prácticas de seguridad por lo que puede ser abordada de manera específica.

Esto se logrará mediante la implementación de una campaña de concientización en redes sociales que se enfoque en la seguridad de la información dentro de la universidad (UPTC).

El objetivo de esta campaña es concientizar a la comunidad upetecista sobre prácticas seguras en línea, destacando de esta forma la importancia de contraseñas seguras y el uso responsable de la Tecnología.

ACTIVIDAD 3: ENTREGAR

En cumplimiento con los objetivos establecidos en este plan se presentan los resultados correspondientes a las actividades realizadas dentro de la fase de identificación de necesidades, esta etapa fue diseñada para analizar y comprender las demandas actuales y futuras de la comunidad universitaria en relación con los servicios y tecnologías ofrecidas por la Dirección de las TIC.

El objetivo de esta actividad es obtener una perspectiva precisa de las necesidades, percepciones y expectativas de la comunidad universitaria. La información que describiremos a continuación nos permitirá diseñar estrategias de comunicación y sensibilización efectivas que aborden de manera específica cada uno de los desafíos y oportunidades identificados en la Universidad.

5.1.2 FASE DE DESARROLLO

La fase de desarrollo del plan de comunicación y sensibilización de la dirección de Tecnologías de la Información implica la transformación de la estrategia conceptual en acciones concretas, esta etapa es esencial para cambiar los objetivos identificados en la fase de identificación de necesidades en iniciativas efectivas.

PUBLICO OBJETIVO

El público objetivo en el plan de comunicación y sensibilización de la Dirección de las Tecnologías de la Información y Comunicación (TIC) en la UPTC debe estar claramente definido para adaptar las estrategias de manera efectiva, por lo tanto, nuestro público será:

- Docentes
- Administrativos
- Estudiantes

Comunidad Universitaria

Para poder involucrar a la comunidad en este plan se pueden implementar diversas estrategias entre las cuales podemos incluir:

- Organizar campañas educativas que destaquen la importancia de la seguridad de la información y las buenas prácticas en el uso de las TIC.
- Realizar talleres que aborden temas específicos, como seguridad cibernética, uso responsable de redes sociales y protección de datos.
- Utilizar diversos canales de comunicación tales como boletines, sitios web, redes sociales para compartir información relevante sobre seguridad.
- Recopilar retroalimentación de la comunidad para mejorar continuamente las estrategias de comunicación y sensibilización.

Mediante el proceso de implementación del plan de comunicaciones, la fase de desarrollo desempeña un papel muy importante al transformar las actividades conceptualizadas durante la fase de diseño en acciones tangibles y efectivas, este periodo estratégico marca la transición desde la planificación teórica hasta la ejecución práctica. A continuación, se darán a conocer cada una de las actividades planeadas en la fase anterior de manera detallada.

ENCUESTA COMUNIDAD UNIVERSITARIA

"Tecnologías de la Información (TI) en la UPTC."

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

1. Tipo de usuario:

   Estudiante
   Docente
   ☐ Administrativo
   Egresados
   Otro:

2. A qué sede te encuentras inscrito:

   Tunja
   ☐ Duitama
   ☐ Sogamoso
   Chiquinquirá
   Otro

3. Como calificarías tu nivel de conocimiento en Tecnologías de la Información:

   Bajo
   Moderado
   Alto

4. Consideras que es importante tener conocimientos sobre las Tecnologías de la Información (TI):

   Si
   No

5. Por favor, indica las áreas de interés en Tecnologías de la Información (TI) en las que te gustaría recibir capacitación, seleccionando todas las opciones que te interesen:

☐ Seguridad de la información
Servicios de TI
Gobierno Digital
Ley 1712/2014 y decreto 1081/2015
Decreto 1519 / 2020
Tips de Seguridad
Política y objetivos de SGSI
Política y objetivos de SGS
Catálogo de servicios
Ciberseguridad
Otro
¿Cuál?

6. ¿Cuáles tu modalidad de aprendizaje preferida?

Presencial
Virtual
Mixta (presencial y virtual)

7. ¿Cuál es tu disponibilidad horaria para participar en las sesiones de aprendizaje en Tecnologías de la Información (TI)?:

Mañana
Tarde

8. ¿Cómo prefieres que sean transmitidos los conocimientos de Tecnologías de la Información?

Talleres prácticos
Inducción y reinducción
Videos
Presentación

Publicaciones correo electrónico
Banners en la página web
Folletos
Otros
¿Cuál?

9. ¿Conqué frecuencia te gustaría recibir esta información?

☐ Trimestral
☐ Semestral
Anual

10. Si tienes alguna otra preferencia o comentario adicional sobre las capacitaciones en TI que te gustaría compartir con nosotros, por favor háznoslo saber.

_____

_____

¡Agradecemos tu participación y colaboración! Tu opinión es muy valiosa para nosotros y nos ayudarán a diseñar programas de capacitación que se ajusten a tus necesidades y expectativas.

Atentamente,

DIRECCION DE LAS TECNOLOGIASY SISTEMAS DE INFORMACION
Y DE LAS COMUNICACIONES

SENSIBILIZACION A LA COMUNIDAD UNIVERSITARIA

Campaña N° 1:

“Contraseñas fuertes, seguridad sólida”

Objetivo de la campaña: promover la conciencia en la comunidad UPTC sobre la importancia de tener contraseñas seguras para proteger la información personal y profesional

MENSAJES CLAVE DE LA PUBLICACION:

Guardianes Digitales: "las contraseñas son la primera liena de defenza contra las amenazas ciberneticas. asegurate que la tuya sea fuerte y unica"

Fuerza de la diversidad: "Emplea contraseñas diferentes para cada cuenta, evita la vulnerabilidad en general "

Actualiza y evoluciona:"Cambia tus contraseñas frecuentemente, de esta manera tendras una seguridad solida"

La formula magica: "Combina mayusculas y minusculas, numeros y caracteres especiales que sean dificiles de averiguar"

Identidad protegida: "Tu contraseña es tu identidad en linea, mantenla segura para proteger no solo tu formacion personal sino el bienestar de toda la comunidad".

CANALES DE COMUNICACIÓN:

Redes sociales: Publicar estos mensajes informativos y consejos de seguridad tanto en las redes sociales de la UPTC como las de la Dirección de Tecnologías (DTIC).

Correo electrónico institucional: Enviar correos informativos a toda la comunidad universitaria (estudiantes, docentes, y personal administrativo) resaltando la relevancia de contraseñas seguras

Poster y Carteles: Colocar poster en lugares estratégicos de la universidad para recordar la importancia de contraseñas fuertes.

Página web de la universidad: Utilizar la pagina web de la universidad como plataforma central para compartir información sobre la campaña

Boletines institucionales: Aprovecha los boletines institucionales para difundir mensajes institucionales

Campaña N° 2:

“Alerta Phishing: protege tu identidad digital en la UPTC”

Objetivo de la campaña: Crear conciencia en la comunidad Universitaria sobre los riesgos del phishing y proporcionar conocimientos prácticos para identificar correos electrónicos sospechosos.

MENSAJES CLAVE DE LA PUBLICACION:

¡Tu conocimiento, tu defensa!

“aprende a identificar correos electrónicos de phishing para proteger tu información personal y académica”

¡Reporta, no respondas!

“Si sospechas de un correo electrónico, repórtalo a la dependencia pertinente en lugar de interactuar con él”.

¡No caigas en la trampa!

“Se prudente al hacer clic en enlaces o proporcionar información sensible, verifica siempre la autenticidad de los correos

¡Comunidad protegida!

“Cada miembro de la UPTC contribuye a la seguridad colectiva al estar alerta ante posibles intentos de

CANALES DE COMUNICACIÓN:

Poster y carteles: Colocar posters en lugares estratégicos de la universidad para recordar a todos la importancia de contraseñas fuertes.

Boletines institucionales: Aprovecha los boletines institucionales para difundir mensajes clave

Página web de la universidad: utilizar la página web de la Universidad como plataforma central para compartir información sobre la campaña

Redes sociales: Publicar estos mensajes informativos y consejos de seguridad tanto en las redes sociales de la UPTC como las de la Dirección de Tecnologías (DTIC).

Correo electrónico institucional: Enviar correos informativos a toda la comunidad universitaria (estudiantes, docentes y personal administrativo) resaltando la relevancia de contraseñas seguras.

Campaña N° 3

“Conectados con responsabilidad: UPTC segura en la red”

Objetivo de la campaña: promover practicas seguras en Internet entre la comunidad Universitaria, fortaleciendo la protección y seguridad personal e institucional.

MENSAJES CLAVE DE LA PUBLICACION:

Software actualizado, riesgos reducidos: “Mantén tus aplicaciones y sistemas actualizados, las actualizaciones suelenincluir parches de seguridad fundamentales.”

Contraseñas fuertes, comunidad protegida: “adopta contraseñas sólidas y únicas, tu seguridad contribuye a la fortaleza digital de toda la comunidad Upetecista”.

Protege tu identidad digital: “resguarda tus datos personales y académicos. La seguridad de tu información comienza contigo”

WIFI segura: “conéctate solo a redes WI-FI seguras, evita el uso de redes públicas para acceder a información sensible”.

CANALES DE COMUNICACIÓN:

Página web de la universidad: utilizar la página web de la Universidad como plataforma central para compartir información sobre la

Poster y carteles: Colocar posters en lugares estratégicos de la universidad para recordar a todos la importancia de contraseñas fuertes.

Redes sociales: Publicar estos mensajes informativos y consejos de seguridad tanto en las redes sociales de la UPTC como las de la Dirección de Tecnologías

Enviar correos informativos a toda la comunidad universitaria (estudiantes, docentes y personal administrativo) resaltando la relevancia de contraseñas seguras.

Boletines institucionales: Aprovecha los boletines institucionales para difundir

Campaña N° 4

“Respalda tu conocimiento: seguridad en los datos de la UPTC”

Objetivo de la campaña: Promover la conciencia sobre la importancia de realizar copias de seguridad (Backups) y la recuperación de información dentro de la comunidad Universitaria, garantizando la seguridad y disponibilidad de los datos. Para realizar las copias de seguridad la dirección de Tecnologías de la Información ha realizado un documento que te guiara en la realización de las copias (A-RI-P03-G01).

MENSAJES CLAVE DE LA PUBLICACION:

Precaución, ante todo: “Realiza copias de seguridad regularmente para proteger tus datos ante posibles pérdidas o daños.”

Recuperación eficaz: “Tener un plan de recuperación de datos en caso de emergencia es esencial para restaurar la información de manera rápida y eficiente”

Responsabilidad compartida: “Todos los miembros de la comunidad tienen la responsabilidad de proteger y respaldar la información relevante para la universidad”.

Prevención de perdidas: “La realización de backups es fundamental para prevenir la pérdida de información valiosa debido a fallos técnicos, errores humanos o ataques cibernéticos.”.

CANALES DE COMUNICACIÓN:

- Publicar estos mensajes informativos y consejos de seguridad tanto en las redes sociales de la UPTC como las de la Dirección de Tecnologías (DTIC).
- Enviar correos informativos a toda la comunidad universitaria (estudiantes, docentes y personal administrativo) resaltando la relevancia de contraseñas seguras.
- Colocar posters en lugares estratégicos de la universidad para recordar a todos la importancia de contraseñas fuertes.
- Utilizar la página web de la Universidad como plataforma central para compartir información sobre la campaña
- Boletines Institucionales
- Aprovecha los boletines para difundir mensajes claves

Al fomentar la participación y crear conciencia sobre la importancia de las tecnologías de manera responsable y segura, la Dirección de las Tecnologías puede contribuir significativamente a un entorno digital más seguro y productivo en la UPTC.

Durante la fase de desarrollo del plan de comunicaciones y sensibilización para la Dirección de Tecnologías de la UPTC es fundamental establecer metas específicas que orienten la implementación efectiva de las estrategias.

METAS

Meta 1: Realización de copias de seguridad

La Dirección de Tecnologías y Sistemas de Información y de las Comunicaciones cuenta con el procedimiento A-RI-P03 Copias de Seguridad de la Información, en donde se definen los pasos a realizar para generar las copias de seguridad de las bases de datos.

Respecto a la información que se encuentre alojada en los equipos de cómputo o PC, el Manual de Políticas de Seguridad de la Información, define que los usuarios son los dueños o custodios y por ende son los responsables de realizar los backup de su propia documentación

Meta 2: Disminución de los incidentes de seguridad que atentan contra la integridad, disponibilidad y confidencialidad de la información.

La Universidad cuenta con el sistema de mesa de servicio en el cual los usuarios de la universidad pueden ingresar y registrar sus incidencias y peticiones, las cuales serán resueltas por un técnico o funcionario encargado, en un tiempo determinado. Luego de que los usuarios realicen el proceso en la mesa de servicios, la dirección de TIC de manera trimestral en el sistema SIPEF hace la medición de los indicadores, y se evidencia cuantos incidentes de seguridad de la información se presentaron en dicho periodo, lo cual permitirá hacer una evaluación de cumplimiento de esta meta.

Meta 3: Cumplimiento al 100% de la política de acceso lógico a los sistemas de información

La universidad cuenta con la política de acceso a los sistemas de información y con los controles específicos para el ingreso a los mismos.

Política de acceso a los sistemas de información:

“El control de acceso a todos los Sistemas de Información de la Universidad y en general cualquier servicio de Tecnologías de Información, debe realizarse por medio de Credenciales de Acceso (Usuario y Contraseña), las cuales son de uso exclusivo e intransferible.

Para la asignación y/o eliminación de credenciales de acceso de usuarios institucionales administrativos, docentes y contratistas se hará de acuerdo al procedimiento de vinculación de servidores públicos A-GH-P03 y entrega de cargos A-GH-P05, y se tendrá en cuenta los lineamientos por la Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones en el procedimiento de Gestión de Identidad y Acceso A-RI-P20.

El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de la UPTC, debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y de la Institución, que se definan por las diferentes dependencias de la Universidad, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.

El acceso lógico a equipo especializado de cómputo (Servidores, enrutadores, bases de datos, etc.) conectado a la red es administrado por la Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones.

La asignación de la contraseña para acceso a sistemas, se debe realizar de forma individual, por lo que el uso de contraseñas compartidas está prohibido. Al revelar o compartir la contraseña el usuario autorizado se expone a responsabilizarse de acciones que otras personas hagan con su contraseña.

Los usuarios son responsables de todas las actividades llevadas a cabo con su identificación de usuario y contraseña.

Es responsabilidad de los usuarios la privacidad de las contraseñas, por lo tanto, se recomienda no registrarlas en ningún medio impreso o escrito en el área de trabajo del usuario, ni almacenarlas en programas o sistemas, con el fin de evitar que las personas no autorizadas tengan conocimiento de las mismas.

Los usuarios deben tener en cuenta las siguientes características para la construcción de sus contraseñas: Que contenga mínimo ocho (8) caracteres, los cuales deben incluir letras mayúsculas, minúsculas, números y símbolos o caracteres especiales y que no contenga información de tipo personal (nombres, numero de documento, fecha de nacimiento, número de teléfono, entre otros).

Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, tendrá la obligación de cambiarla inmediatamente.

La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones debe implementar en las bases de datos un límite de intentos consecutivos infructuosos para ingresar la contraseña.”

Meta 4: Personal sensibilizado y capacitado en buenas prácticas de seguridad de la información.

Objetivo	Que comunica	Frecuencia	Quien comunica (responsable)	Estrategia de comunicación (Medios)	Grupos de interés
Dar a conocer el uso y los beneficios que plantea el Gobierno nacional con la iniciativa de datos abiertos.	Información relevante para la comunidad universitaria del uso y apropiación de datos abiertos.	Semestralmente	Funcionario asignado DTIC	Portal web - Micrositio de Gobierno Digital Redes sociales Correo Institucional Boletines Institucionales	Toda la Comunidad Universitaria y ciudadanía en general
Dar a conocer la ley 1712 de 2014 Transparencia y acceso a la Información pública con el fin de generar una cultura de transparencia, legalidad e Integridad en la Universidad.	Ley 1712 de 2014 Transparencia y acceso a la Información pública y su Decreto reglamentario 1081 de 2015.	Semestralmente	Funcionario asignado DTIC	Portal Web - Micrositio de Transparencia y acceso a la Información - Micrositio de DTIC Correo Institucional (Masivo), Redes Sociales.	Toda la Comunidad Universitaria y ciudadanía en general
Socializar los procedimientos del Proceso Gestión de Recursos Informáticos - RI	Uso, apropiación y Actualización de los procedimientos del proceso Gestión de Recursos Informáticos.	Cuando sea requerido	Funcionario asignado DTIC	Mapa de Proceso de SIG, Capacitación, Correo Institucional, Inducción puestos de trabajo	Personal DTIC Tunja Personal DTIC Duitama Personal DTIC Sogamoso Personal DTIC Chiquinquirá
				Inducción a estudiantes Docente, primero y segundo semestre .	Estudiantes y Docentes
		Semestralmente	Funcionario asignado DTIC	Inducción Reinducción	Personal Administrativo

Objetivo	Que comunica	Frecuencia	Quien comunica (responsable)	Estrategia de comunicación (Medios)	Grupos de interés
Dar a conocer la Estratégica Misional y la Visión de la operaciones de la Dirección de Tecnologías, los diferentes lineamientos y directrices gestionados alrededor tecnológica de información y de las comunicaciones y adoptados en el Universidad, así mismo recordar a la comunidad universitaria los servicios que DTIC ofrece en su catálogo de Servicio	Quienes somos, la Misión y Visión, Objetivos, políticas, Información de Interés, Normativa, organigrama y generalidades de la Dirección de las Tecnologías.	Semestralmente	Funcionario asignado DTIC	Página Web Micrositio de DTIC Correo institucional Boletines Institucionales	Toda la Comunidad Universitaria
				Inducción a estudiantes primer semestre	Estudiantes
				Inducción y reinducción a funcionarios	Personal Administrativo
				Mapa de Proceso de SIG	
		Cuando sea requerido		Inducción puestos de trabajo	Personal DTIC Tunja Personal DTIC Duitama Personal DTIC Sogamoso Personal DTIC Chiquinquirá
				Mapa de Proceso de SIG	
Socializar información relevante relacionada con SGS y SGSI	Tips de seguridad	Semestral	Funcionario asignado DTIC	Página Web Micrositio de DTIC Correo institucional Boletines Institucionales	Personal administrativo, Docentes, Estudiantes y proveedores
				Redes Sociales institucionales Pantallas de la Universidad Capacitación Inducción y Reinducción	
	Seguimiento a la mejora continua SGS y SGSI	Trimestral		Taller de Gestión Sistema Plan de Mejora Correo	Alta dirección
	Objetivos del SGS Objetivos del SGSI Manual de Políticas del SGSI Política del SGS Política del SGSI Plan del SGS - SGSI Plan del SGS - SGSI	Anual		Inducción Reinducción Redes sociales Institucionales Taller de Gestión Contrato Sistema SIG	Comunidad universitaria Proveedores Personal DTIC Tunja Personal DTIC Duitama Personal DTIC Sogamoso Personal DTIC Chiquinquirá Toda la Comunidad Universitaria

Dar a conocer los objetivos y la política de gobierno digital	objetivos de gobierno digital	Anualmente	Funcionario asignado DTIC	capacitación	Comunidad universitaria en general
	Política de gobierno digital	Anualmente	Funcionario asignado DTIC	capacitación	Comunidad universitaria en general
Dar a conocer las estrategias de gobierno digital	Estrategias para el fortalecimiento ciudadano-estado, con miras a mejorar la prestación de los servicios por parte de la universidad	semestralmente	Funcionario asignado DTIC	Redes sociales	Comunidad universitaria en general

Meta 5: Capacitar y sensibilizar alos funcionarios de las sedes en el sistema de Gestión de Seguridad de la Información.

Las coordinadoras de las sedes seccionales Duitama, Sogamoso y Chiquinquirá, deberán realizar cada una un plan de comunicaciones, donde se especifique que se ejecutarán capacitaciones y sensibilizaciones a los funcionarios de las mismas.

5.1.3 FASE DE IMPLEMENTACION

5.1.3.1 Socialización del plan con la alta dirección

La socialización del plan de comunicaciones con la alta dirección es un proceso fundamental y estratégico para garantizar el cumplimiento de los objetivos y la obtención de su respaldo, durante esta socialización se presentarán de manera detallada las estrategias y acciones propuestas dentro del plan, destacando su relevancia para el logro de los objetivos institucionales y la mejora de la imagen de la organización.

5.1.4 Técnicas recomendadas para comunicación de información

entro de esta fase se llevará a cabo la ejecución concreta de las estrategias establecidas en las fases anteriores, a continuación, describiremos las actividades a realizar de una manera detallada.

Se dará inicio a las actividades de comunicación, que pueden incluir la distribución de materiales impresos, la implementación de campañas en línea, organización de talleres prácticos, elaboración de videos, presentaciones entre otras actividades, las cuales nos ayudaran a generar conciencia sobre las iniciativas tecnológicas y sus beneficios.

Dentro de las actividades proyectadas en el plan de comunicación y sensibilización de la Dirección de Tecnologías de la UPTC se encuentran:

TALLERES PRÁCTICOS PARA ESTUDIANTES, DOCENTES Y ADMINISTRATIVOS

- **TALLER #1 MANEJO DE DATOS SENSIBLES**.

El objetivo de este taller es sensibilizar y capacitar a la comunidad universitaria sobre la importancia del manejo seguro de datos sensibles, promoviendo buenas prácticas para la protección de la información institucional.

- **TALLER #2 SEGURIDAD EN LAS ESTACIONES DE TRABAJO "PANTALLA LIMPIA".**

El objetivo de este taller es concientizar a la comunidad universitaria sobre las mejores prácticas de seguridad relacionadas con la "pantalla limpia", enfocándonos en la protección de información sensible y la prevención de accesos no autorizados.

CAPACITACIÓN A COMUNIDAD UNIVERSITARIA SOBRE LA IMPORTANCIA DE MARCAR LOS CORREOS SPAM

Es una práctica importante para fortalecer la seguridad y proteger la integridad de las cuentas de correo electrónico.

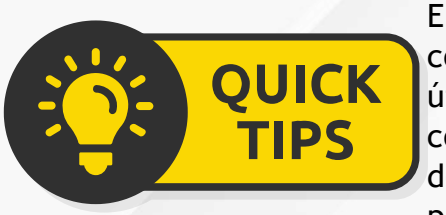
SOCIALIZACIÓN “EXPLORANDO LOS SERVICIOS DE TI EN LA UPTC”

El objetivo de esta actividad es informar y destacar la variedad de servicios de TI que la Dirección de Tecnologías ofrece a la comunidad universitaria.

PRESENTACIÓN “FORTALECIENDO LA CIBERSEGURIDAD EN LA UPTC”

El objetivo de esta actividad es concientizar y capacitar a la comunidad universitaria sobre la importancia de la ciberseguridad, de igual forma proporcionar pautas para fortalecer la seguridad digital en la universidad.

PUBLICACIÓN “TIPS DE SEGURIDADEN LA UPTC”



El objetivo principal de esta actividad es proporcionar a la comunidad universitaria de la UPTC información practica y útil sobre seguridad digital, la meta es fortalecer la conciencia y las prácticas de seguridad entre estudiantes, docentes y personal administrativo, contribuyendo así a la protección de datos y la prevención de posibles amenazas cibernéticas.

5.1.5 FASE DE MEJORAMIENTO

El objetivo de la fase de mejoramiento del plan de comunicación y sensibilización en la Dirección de Tecnologías de la UPTC es optimizar y fortalecer las estrategias existentes para lograr una implementación más efectiva y una mayor participación de toda la comunidad.

Dentro de algunas otras acciones planificadas se tienen las siguientes:

Realizar una revisión de las estrategias de comunicación y sensibilización implementadas hasta la fecha mediante la recopilación de comentarios, entrevistas y retroalimentación del personal involucrado en el plan.

Analizar los resultados obtenidos durante el desarrollo del plan para lograr identificar temas específicos que requieran mejoras.

Implementar nuevas estrategias de comunicación de acuerdo a las revisiones realizadas o a las contingencias que se puedan presentar en la presente vigencia

Esta fase de mejoramiento del plan de comunicación está diseñada para ser un proceso iterativo, donde la retroalimentación y la flexibilidad son clave para ajustarse a las necesidades cambiantes de la Universidad y del entorno tecnológico.

Objetivos de la Mejora

- Mejorar el plan de comunicaciones de la Dirección de Tecnologías de la UPTC implica una serie de objetivos que buscan fortalecer la efectividad y eficiencia de las comunicaciones dentro de la Universidad.

- Mejorar la difusión de información: Asegurarse de que toda la información relevante se comunique de manera clara y oportuna a todos los interesados, incluyendo estudiantes, profesores, personal administrativo y directivos.

- Incrementar la transparencia: Promover una cultura de transparencia mediante la comunicación abierta y honesta sobre los logros enfrentados y los alcanzados por la Dirección de Tecnologías.

- Facilitar la colaboración: Fomentar la colaboración entre diferentes áreas y departamentos dentro de la universidad mediante una comunicación efectiva que promueva la integración de ideas y la resolución conjunta de problemas.

- Optimizar los canales de comunicación: Evaluar y mejorar los canales de comunicación existentes, como correos electrónicos, boletines, reuniones, plataformas en línea, redes sociales, entre otros, para garantizar la difusión de la información.

- Promover la seguridad de la información: Educar a la comunidad universitaria sobre las mejores prácticas de seguridad de la información a través de campañas de concientización y comunicación regular sobre políticas y procedimientos de seguridad.

GLOSARIO

- Brecha: Se denomina al espacio o ruta a recorrer entre un estado actual y un estado deseado

- Difundir: Propagar o divulgar conocimiento, programas, actividades y resultados académicos y el impacto de los proyectos de extensión, etc.

- Entrenamiento: Proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo.

- Estrategia: Es el camino para seguir por una organización para el logro de sus metas y objetivos.

- Estrategia de Comunicación: Es el conjunto de prácticas e instrumentos de intercambio comunicacional dirigidos a mostrar una realidad nueva (informar), cuestionar y revisar lo previo (generar opinión), modificar prácticas y actitudes (tomar decisiones).

- Extensión: Es una función misional y sustantiva de la Universidad, a través de la cual se establece una interacción privilegiada y recíproca entre el conocimiento sistemático de la academia y los saberes y necesidades de la sociedad, y de las organizaciones e instituciones que hacen parte de ella. Esta relación entre la Universidad y su entorno se debe reflejar en la ampliación del espacio de deliberación democrática y en el bienestar de las comunidades. Con la Extensión se cualifican la ciencia, la tecnología, el arte y la cultura.

- Ingeniería Social: “Tipo de ataque de seguridad en la cual un individuo manipula al otro con el fin de obtener información que puede ser utilizada para acceder a un sistema no autorizado, sustraer dinero o incluso suplantar la identidad de la víctima”.

- Política: Declaraciones de alto nivel que expresan los objetivos a cumplir de la Entidad respecto a algún tema en particular.

- Proyecto: Un proyecto, como unidad operativa mínima de un plan, se define como un conjunto de actividades planificadas, concretas y relacionadas entre sí, que vinculan tiempo y recursos específicos para lograr un objetivo y unas metas definidas.

- Plan de Comunicación: Herramienta que permite planificar (en términos de recursos, tiempo y objetivos), las acciones y estrategias de comunicación de la Universidad.

- Sensibilización: Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

V.B. LEONARDO BERNAL ZAMORA

Director de las Tecnologías y Sistemas de Información y de las Comunicaciones
Líder del Proceso
Representante ante la alta Dirección de las Normas ISO 20001:2018 e ISO 27001:2022

Proyectó: *Equipo de Gestión TI y Gobierno DTIC*