PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones
UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA

PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Tabla de contenido

PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Introducción

En la última década, las tecnologías de información y comunicaciones se han convertido en la herramienta por excelencia para la optimización de los procesos y el funcionamiento eficaz de las empresas.

Con el uso de la tecnología, surgen a su vez amenazas y vulnerabilidades asociadas, que pueden llegar a afectar la disponibilidad, privacidad, confidencialidad e integridad de la información que se encuentra en las diferentes plataformas, afectando de esta manera el desempeño normal de la Entidad.

Para esto, el MODELO DE SEGURIDAD Y PRIVACIDAD indica pautas específicas para guiar a las instituciones a mejorar sus plataformas y mitigar amenazas que pueden llegar a traer consigo las tecnologías implementadas, sin embargo, un programa robusto de seguridad y privacidad de la información, no se basa únicamente en el aseguramiento de plataformas y procesos, sino que también debe involucrar los factores humanos, que en muchos casos, son la principal causa de los incidentes de seguridad dentro de un sistema determinado, esto debido a que no conocen sobre seguridad de la información y su rol dentro de la Entidad.

Muchas instituciones no prestan la suficiente atención a su recurso humano, que puede llegar a ser el eslabón más débil en la cadena de la seguridad de la información, por lo que es necesario sensibilizarlos o capacitarlos sobre la importancia de la preservación de la información.

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

PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

Realizar estrategias de comunicaciones para dar a conocer los aspectos más importantes que realiza la Dirección de Tecnologías en cumplimiento de las normas ISO 27001:2013 e ISO 20000-1:2018, para así asegurar que se cubra en su totalidad los funcionarios de la Entidad, asegurando que cada uno cumpla con sus roles y responsabilidades de seguridad y privacidad de la información dentro de la Universidad.

PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

2. ALCANCE

El Alcance del Plan de capacitación, sensibilización y comunicación de la seguridad de la información de la Dirección de las Tecnologías de la Información y de las Comunicaciones de la Universidad Pedagógica y Tecnológica de Colombia es gestionar las estrategias de comunicación para toda la comunidad.

3. ROLES Y RESPONSABILIDADES

El acta de roles y responsabilidades se encuentra publicada en el link:

4. FASES DEL PLAN

DISEÑO	• indentifica las tareas a ser realizadas para cumplir con las metas establecidas por la universidad.
DESARROLLO	• Se enfoca en las fuentes de información disponibles, alcance y contenidos del material de entrenamiento.
IMPLEMENTACION	• Direcciona efectivamente la manera como deberá comunicarse el material diseñado
MEJORAMIENTO	• Indica como mantener el sistema actualizado monitoreando su efectividad.

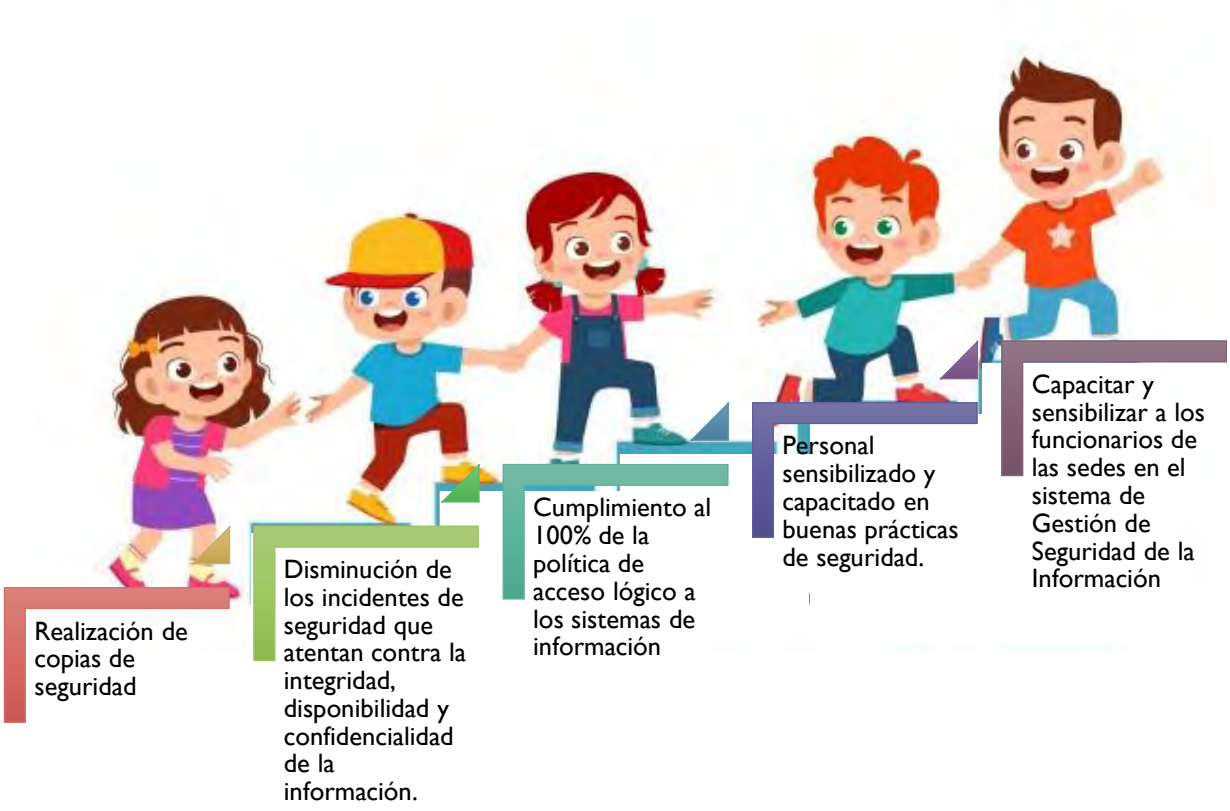
Figura 1. Fases plan de sensibilización, capacitación y comunicación

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

PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.1 Fase de Diseño

4.1.1 Metas



4.1.2 Tareas

ACTIVIDAD 1: CAPACITAR

Busca asegurar que los usuarios desde el más principiante hasta el más experimentado, tengan los conocimientos suficientes para desempeñar sus roles. Esto se logra a través de capacitaciones, charlas, videos, tips de seguridad y demás estrategias que hagan que los funcionarios despierten el interés en seguridad de la información, algunas otras relacionadas con conceptos de seguridad de la información.

ACTIVIDAD 2: SENSIBILIZAR

Impactar sobre el comportamiento de la comunidad universitaria, reforzando las buenas prácticas sobre seguridad de la información, inculcando las políticas y la importancia del Sistema de Gestión de Seguridad de la información.

ACTIVIDAD 3: ENTREGAR

Busca enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas a su cargo, respecto a la seguridad de la información.

4.2 Fase de Desarrollo

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.

PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

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 SIPEF, en donde de forma semestral se 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.

PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

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 debe comunicar (Responsable)	Estrategia de comunicación	Grupos de Interés (A quien Comunica)
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	Banner portal Web Redes sociales Correo institucional	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 un 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	Correo Institucional Masivo, Redes Sociales.	Toda la Comunidad Universitaria y ciudadanía en general

PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo	Que comunica	Frecuencia	Quien debe comunicar (Responsable)	Estrategia de comunicación	Grupos de Interés (A quien Comunica)
Socializar los procedimientos del proceso Gestión de Recursos Informáticos	Uso, apropiación y Actualización de los procedimientos del proceso Gestión de Recursos Informáticos	Cuando sea requerido o necesario	Funcionario asignado DTIC	Capacitación Inducción puestos de trabajo	Personal DTIC Tunja Personal DTIC Duitama Personal DTIC Sogamoso Personal DTIC Chiquinquirá
		Semestralmente	Funcionario asignado DTIC	Inducción a estudiantes primero y segundo semestre 2022	Estudiantes
				Inducción Reinducción	Personal Administrativo
Dar a conocer y recordar a la comunidad universitaria los servicios que DTIC ofrece en su catálogo de Servicio	Objetivos y generalidades de los servicios del catálogo	Semestralmente	Funcionario asignado DTIC	Inducción a estudiantes primer semestre 2022	Estudiantes
				Inducción y reinducción a funcionarios Sistema SIG	Personal Administrativo
		Cuando sea requerido		Inducción puestos de trabajo Sistema SIG	Personal DTIC Tunja Personal DTIC Duitama Personal DTIC Sogamoso Personal DTIC Chiquinquirá

PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo	Que comunica	Frecuencia	Quien debe comunicar	Estrategia de comunicación	Grupos de Interés
Socializar información relevante relacionada con SGS y SGSI	Tips de Seguridad	Semestralmente	Director y/o funcionario asignado DTIC	Correo Página web Redes Sociales institucionales Pantallas de la Universidad Capacitación Inducción y Reinducción	Personal Administrativo Comunidad universitaria en general
	Seguimiento a la mejora continua SGS y SGSI	Trimestralmente		Taller de Gestión Sistema Plan de Mejora	Alta Dirección
	Objetivos del SGS	Anual		Correo 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
	Objetivos del SGSI				
	Manual de Políticas del SGSI				
	Política del SGS				
	Política del SGSI				
	Plan del SGS - SGSI				

Meta 5: Capacitar y sensibilizar a los 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.

4.3 Fase de Implementación

Se realizarán las actividades de sensibilización y capacitación teniendo en cuenta las siguientes estrategias de comunicación:

- Banner
- Portal web
- Micro sitio de la Dirección
- Micro sitio de Gobierno en línea
- Redes sociales institucionales
- Correo Institucional Masivo
- Inducción a estudiantes primero y segundo semestre
- Capacitación
- Inducción puestos de trabajo
- Rally (organizado por el SIG)
- Sistema SIG
- Procedimientos del Proceso
- Talleres de Gestión
- Sistema SIPEF
- Rendición de cuentas
- Informe a la alta dirección
- Acuerdos de nivel de servicio con proveedores

4.4 Fase de Mejoramiento

Las acciones de mejora se deben comunicar a todas las partes interesadas, con un nivel de detalle apropiado a las circunstancias y en donde sea pertinente llegar a acuerdos sobre cómo proceder.

Evaluación: Para evaluar las capacitaciones se tendrá en cuenta el formulario de satisfacción luego de cada capacitación realizada.

PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.4.1 Objetivos de la Mejora

Calidad:

Mejorar continuamente la gestión hacia su modernización, bajo un marco de desempeño eficiente, eficaz y efectivo.

Recursos

Asegurar que los recursos de TI para la prestación de los servicios sean respaldados por unas capacidades técnicas, de recurso humano y financieras y cuenten con la tecnología adecuada.

Productividad

Fomentar el uso permanente de nuevas tecnologías de información y comunicación, que permitan la prestación de servicios, cumpliendo con las políticas de seguridad de la información, para la satisfacción de necesidades de los usuarios.

Realizar nuevas estrategias para el mejoramiento continuo en la prestación del servicio de TI.

Reducción de riesgos

Tomar medidas preventivas, correctivas y de mejoramiento que permitan disminuir, controlar y mitigar la materialización de los riesgos.

Capacidad

Determinar los elementos con que se cuentan para prestar los servicios del catálogo de servicios de TI y preservar la seguridad de la información.

Valor

Generar estrategias para asegurar la protección de la información como un activo vital de la organización, e implementar controles para alcanzar un correcto nivel de seguridad y administrar estos controles para mantenerlos y mejorarlos a lo largo del tiempo y así poder prestar los servicios de TI de manera eficiente.

Costo

Buscar y emplear tecnologías libres evitando en lo posible suscripciones anuales, limitando los costos a soporte trabajo – hora y evitar pagos de licencias por uso.

4.4.2 Medición De Las Mejoras Implementadas

Para poder visualizar las mejoras implementadas, es necesario revisar los informes generados de los indicadores de gestión, los cuales se encuentran publicados en el Sistema SIPEF (Modulo Plan de Mejora, Indicadores y Acta Taller de Gestión).

4.4.3 Informar Sobre Las Mejoras Implementadas

Se pueden verificar las mejoras implementadas y los indicadores de las mismas en el sistema SIPEF (Sistema Integrado De Planeación Estratégica Y Financiera), Adicional la información de las mejoras implementadas son dadas a conocer en los talleres de gestión y en apoyo en redes sociales, informe a la alta dirección, correos masivos y página de la universidad si es el caso.

Acción Correctiva

El objetivo de estas acciones es eliminar la causa de problemas asociados con los requisitos del SGSI (Estas no conformidades son el resultado de las auditorías realizadas dentro del seguimiento y revisión del SGSI), con el fin de prevenir que ocurran nuevamente.

- Determinar y evaluar las causas de los problemas del SGSI e incidentes de seguridad de la información.
- Diseñar e implementar la acción correctiva necesaria.
- Revisar la acción correctiva tomada.

PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Acción Preventiva

El objetivo de las acciones preventivas es eliminar la posibilidad de ocurrencia de no conformidades potenciales con los requisitos del SGSI. Los procedimientos necesarios para esta acción son:

- Determinar y evaluar las causas de las no conformidades potenciales.
- Diseñar e implementar la acción preventiva necesaria.
- Revisar la acción preventiva tomada.

Se debe identificar los cambios en los riesgos e identificar los requisitos en cuanto acciones preventivas, enfocando la atención en los riesgos que han cambiado significativamente. De esta manera la prioridad de las acciones preventivas se debe determinar con base en los resultados de la valoración de los riesgos.

Para el cumplimiento de estas acciones se cuenta con el Procedimiento, Acciones Preventivas y Correctivas V-EI-P04 del Sistema Integrado de Gestión.

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).

PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- **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"[1].

- **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.

Firma: **GERMÁN AMÉZQUITA BECERRA**
Director de las Tecnologías y Sistemas de la Información y de las Comunicaciones
Líder de Proceso

Proyectó: Grupo de gestión DTIC