SEGUIMIENTO A LA POLITICA DEL SISTEMA DE GESTIÓN

DE SEGURIDAD DE LA INFORMACIÓN

JUNIO 2021

SISTEMA DE GESTIÒN DE SEGURIDAD DE LA INFORMACIÓN

COMPROMISOS SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. La gestión del riesgo de seguridad de la información, implementando los controles necesarios que permitan proteger la integridad, confidencialidad y disponibilidad de acuerdo con su clasificación.

2. El impulsar una cultura en seguridad y privacidad de la información con las partes interesadas, a través del desarrollo de programas y planes de divulgación, capacitación, entrenamiento y concienciación.

3. El diseñar e implementar servicios de Tecnología con los niveles de disponibilidad y continuidad definidos para que los procesos cumplan sus objetos.

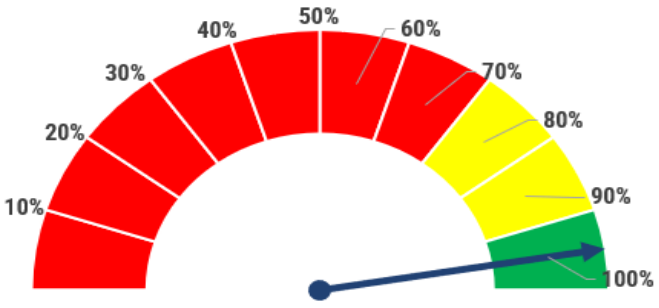
Los compromisos de seguridad de la información se despliegan a través de los siguientes objetivos:

- Implementar los controles del Modelo de Seguridad y Privacidad de la Información - MSPI a partir de los requisitos de seguridad con el propósito de gestionar los riesgos y preservar la confidencialidad, integridad y disponibilidad de los activos de información.
- Promover la cultura de seguridad y privacidad de la información
- Definir y mantener actualizados los servicios de TI que permitan el cumplimiento de los objetivos estratégicos institucionales

RESULTADOS MEDICIÓN DE OBJETIVOS A JUNIO 2021

En el período se evaluaron tres de tres objetivos, a través de 3 indicadores en el período evaluado con los cuáles se tuvo un cumplimiento promedio de **95%** como se muestra en la gráfica 1.

Gráfico 1 Cumplimiento Promedio Objetivos SGSI



Fuente: Elaboración Propia

Nota: El cumplimiento promedio se estableció como el promedio de cumplimiento de cada objetivo.

Este cumplimiento se detalla así:

Tabla 1 Cumplimiento de Metas de los Objetivos SGSI

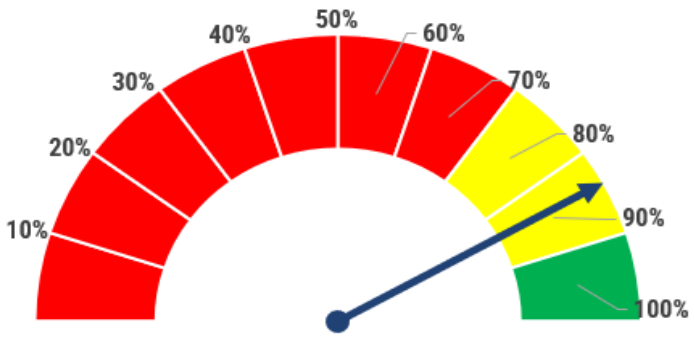
OBJETIVO MIPG-SIG	META	NOMBRE INDICADOR	CUMPLIMIENTO	INDICADOR
Implementar los controles del Modelo de Seguridad y Privacidad de la Información - MSPI a partir de los requisitos de seguridad con el propósito de gestionar los riesgos y preservar la confidencialidad, integridad y disponibilidad de los activos de información.	85%	Nivel de implementación de controles del MSPI	NO CUMPLE	84 %
Promover la cultura de seguridad y privacidad de la información	85%	Nivel de cumplimiento de las actividades de promoción de cultura de seguridad y privacidad de la información	CUMPLE	100%
Definir y mantener actualizados los servicios de TI que permitan el cumplimiento de los objetivos estratégicos institucionales	100%	Actualización del Catálogo de servicios de TI	CUMPLE	100%

Fuente: Elaboración Propia

ANÁLISIS DE RESULTADOS

Objetivo: Implementar los controles del Modelo de Seguridad y Privacidad de la Información - MSPI a partir de los requisitos de seguridad con el propósito de gestionar los riesgos y preservar la confidencialidad, integridad y disponibilidad de los activos de información.

Gráfico 2 Cumplimiento Objetivo 1 SGSI



Fuente: Elaboración Propia

El objetivo tuvo un cumplimiento promedio del **84 %** donde el indicador evaluado en el período cumplió la meta planteada.

- **Nivel de implementación de controles del MSPI**

Tabla 2 Nivel de implementación de controles del MSPI

META	NOMBRE INDICADOR	FORMULA DE CÁLCULO	CUMPLIMIENTO	INDICADOR	Numerador del Indicador	Denominador del Indicador
85%	Nivel de implementación de controles del MSPI	(Número de controles implementados de la declaración de aplicabilidad en el periodo evaluado/ Número total de controles planeados de la declaración de aplicabilidad para el periodo evaluado) *100	NO CUMPLE	84%	27	32

Fuente: Elaboración Propia

A partir de la aprobación, publicación y socialización del manual de políticas específicas de seguridad y privacidad de la información, desde el equipo técnico se empezó a identificar la aplicación de los controles del anexo A de la norma y formalizar su nivel de implementación.

Los controles implementados se relacionan a continuación.

UNIDAD NACIONAL DE PROTECCION

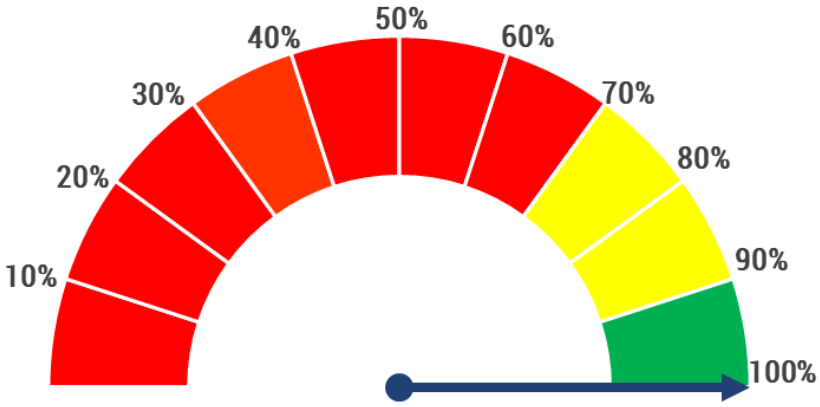
DECLARACIÓN DE APLICABILIDAD

NTC ISO 27001:2013 Anexo A

# Dominio		# Objetivo	Nombre objetivo	Texto objetivo	# Control	Nombre control	Texto control	Aplicabilidad	Estado
A.5	Políticas de la seguridad de la información	A.5.1	Orientación de la dirección para la gestión de la seguridad de la información	Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	A.5.1.1	Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	SI	IMPLEMENTADO
A.5	Políticas de la seguridad de la información	A.5.1	Orientación de la dirección para la gestión de la seguridad de la información	Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.	SI	IMPLEMENTADO
A.6	Organización de la seguridad de la información	A.6.1	Organización interna	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.	A.6.1.1	Roles y responsabilidades para la seguridad de la información.	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	SI	IMPLEMENTADO
A.6	Organización de la seguridad de la información	A.6.1	Organización interna	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.	A.6.1.2	Separación de deberes.	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	SI	IMPLEMENTADO
A.6	Organización de la seguridad de la información	A.6.2	Dispositivos móviles y teletrabajo	Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles	A.6.2.1	Política para dispositivos móviles	se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	SI	IMPLEMENTADO
A.6	Organización de la seguridad de la información	A.6.2	Dispositivos móviles y teletrabajo	Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles	A.6.2.2	Teletrabajo	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	SI	IMPLEMENTADO
A.7	Seguridad de los recursos humanos	A.7.1	Antes de asumir el empleo	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y éticas pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y los riesgos percibidos.	SI	IMPLEMENTADO
A.7	Seguridad de los recursos humanos	A.7.2	Durante la ejecución del empleo	Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	A.7.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	SI	IMPLEMENTADO
A.7	Seguridad de los recursos humanos	A.7.2	Durante la ejecución del empleo	Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	A.7.2.3	Proceso disciplinario	Se deben contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	SI	IMPLEMENTADO
A.8	Gestión de activos	A.8.1	Responsabilidad por los activos	Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.	A.8.1.1	Inventario de activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	SI	IMPLEMENTADO
A.8	Gestión de activos	A.8.1	Responsabilidad por los activos	Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.	A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.	SI	IMPLEMENTADO
A.9	Control de acceso	A.9.1	Requisitos del negocio para control de acceso	Limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	SI	IMPLEMENTADO
A.9	Control de acceso	A.9.1	Requisitos del negocio para control de acceso	Limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1.2	Acceso a redes y a servicios en red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	SI	IMPLEMENTADO
A.9	Control de acceso	A.9.2	Gestión de acceso de usuarios	Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	A.9.2.2	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	SI	IMPLEMENTADO
A.9	Control de acceso	A.9.2	Gestión de acceso de usuarios	Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	SI	IMPLEMENTADO
A.10	Criptografía	A.10.1	controles criptográficos	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.	A.10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	SI	IMPLEMENTADO
A.11	Seguridad física y del entorno	A.11.1	Áreas seguras	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	A.11.1.1	Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	SI	IMPLEMENTADO
A.11	Seguridad física y del entorno	A.11.2	Equipos	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	A.11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	SI	IMPLEMENTADO
A.11	Seguridad física y del entorno	A.11.2	Equipos	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	A.11.2.2	Servicios de suministros	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	SI	IMPLEMENTADO
A.11	Seguridad física y del entorno	A.11.2	Equipos	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	A.11.2.3	Seguridad del cableado	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	SI	IMPLEMENTADO
A.11	Seguridad física y del entorno	A.11.2	Equipos	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	A.11.2.9	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	SI	IMPLEMENTADO
A.12	Seguridad de las operaciones	A.12.1	Procedimientos operacionales y responsabilidades	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	A.12.1.2	Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	SI	IMPLEMENTADO
A.12	Seguridad de las operaciones	A.12.2	Protección contra códigos maliciosos	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	A.12.2.1	Controles contra códigos maliciosos	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	SI	IMPLEMENTADO
A.12	Seguridad de las operaciones	A.12.4	Registro y seguimiento	Registrar eventos y generar evidencia.	A.12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	SI	IMPLEMENTADO
A.13	Seguridad de las comunicaciones	A.13.1	Gestión de la seguridad de las redes	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	A.13.1.3	Separación de las redes	Los grupos de servicios de información, usuarios y sistema de información se deben separar en las redes.	SI	IMPLEMENTADO
A.14	Adquisición, desarrollo y mantenimiento de sistemas	A.14.2	Seguridad en los procesos de desarrollo y de soporte	Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	A.14.2.1	Política de desarrollo seguro	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	SI	IMPLEMENTADO
A.18	Cumplimiento	A.18.1	Cumplimiento de requisitos legales y contractuales	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamento o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.	SI	IMPLEMENTADO

Objetivo: Promover la cultura de seguridad y privacidad de la información

Gráfico 3 Cumplimiento Promedio Objetivo 2 SGSI



Fuente: Elaboración Propia

El objetivo tuvo un cumplimiento promedio del **100%,** el indicador evaluado en el período cumplió la meta planteada.

- **Nivel de cumplimiento de las actividades de promoción de cultura de seguridad y privacidad de la información**

Tabla 3 Nivel de cumplimiento de las actividades de promoción de cultura de seguridad y privacidad de la información.

META	NOMBRE INDICADOR	FORMULA DE CÁLCULO	CUMPLIMIENTO	INDICADOR	Numerador del Indicador	Denominador del Indicador
85%	Nivel de cumplimiento de las actividades de promoción de cultura de seguridad y privacidad de la información	(Número de actividades realizadas del plan de comunicaciones en el periodo evaluado/ Número de actividades planeadas del plan de comunicaciones para el periodo evaluado) *100	CUMPLE	100%	4	4

Fuente: Elaboración Propia

El plan de seguridad y privacidad de la información está integrado a la estrategia de comunicaciones del Sistema de Gestión, donde se tiene dispuesto desplegar la comunicación para todos los sistemas de gestión.

Sin embargo, desde el equipo técnico de sistemas de gestión de seguridad de la información SGSI, se desarrollaron cuatro actividades complementarias para fortalecer la cultura en seguridad de la información, así:

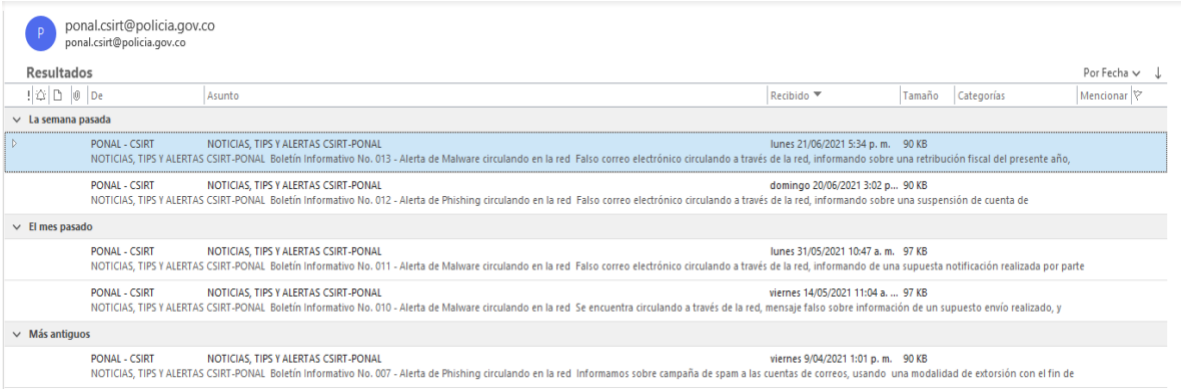
- ✓ Despliegue de boletines relacionados con ciberseguridad
- ✓ Despliegue de boletines de días especiales relacionados con la seguridad de la información.

- ✓ Despliegue de la socialización del Manual de políticas especificas de seguridad y privacidad de la información.
- ✓ Charlas de seguridad de la información.

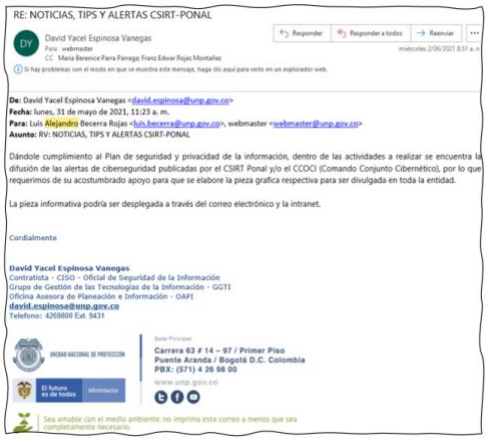
Despliegue de boletines relacionados con ciberseguridad

Desde el csirt Ponal llegaron 5 boletines relacionados con seguridad de la información, los cuales fueron desplegados a interior de la entidad, así:

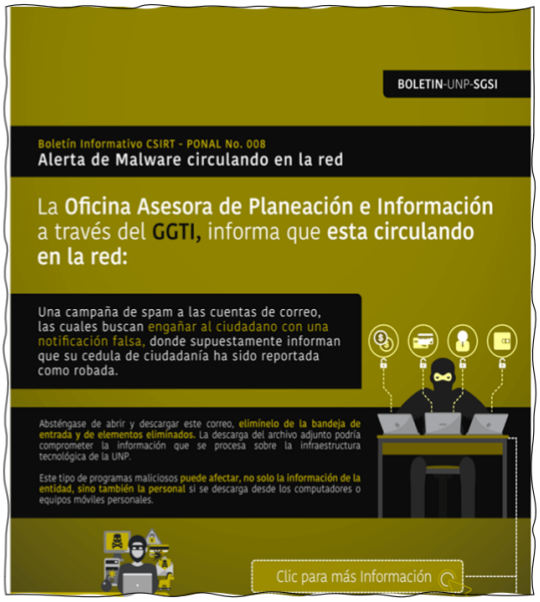
Boletines enviados por el CSIRT Ponal



Correos enviados al Webmaster para el diseño gráfico y posterior divulgación



Despliegue a toda la entidad.



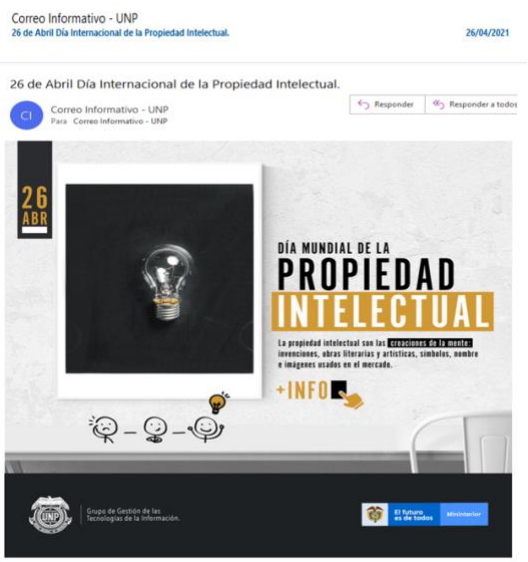
Despliegue de boletines de días especiales relacionados con la seguridad de la información.

Se elaboraron los contenidos para el despliegue de los boletines relacionados con los siguientes días especiales.

- ✓ 26 de abril Dia Internacional de la Propiedad Intelectual

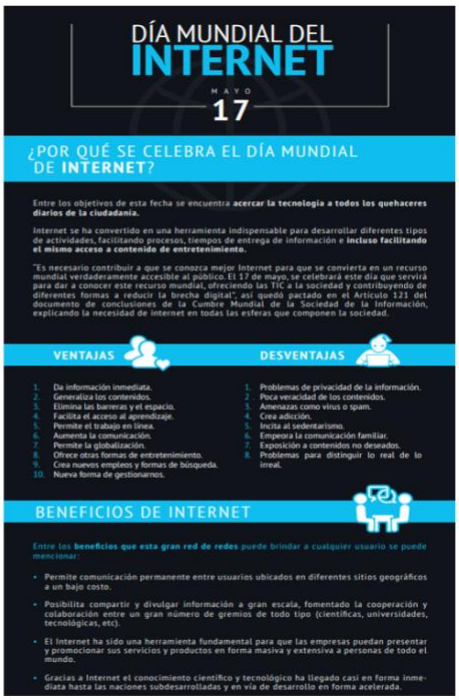
- ✓ 6 de mayo se celebra el día internacional de la contraseña
- ✓ 17 de mayo - día internacional del internet
- ✓ 7 de junio se celebra el día mundial contra la falsificación y la piratería
- ✓ 30 de junio - Dia mundial de las redes sociales

26 de abril Dia Internacional de la Propiedad Intelectual



6 de mayo se celebra el día internacional de la contraseña

17 de mayo - día internacional del internet

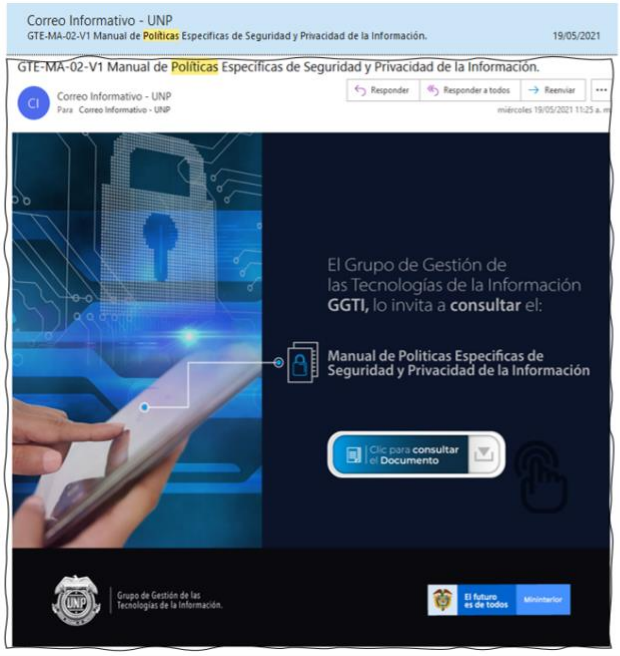


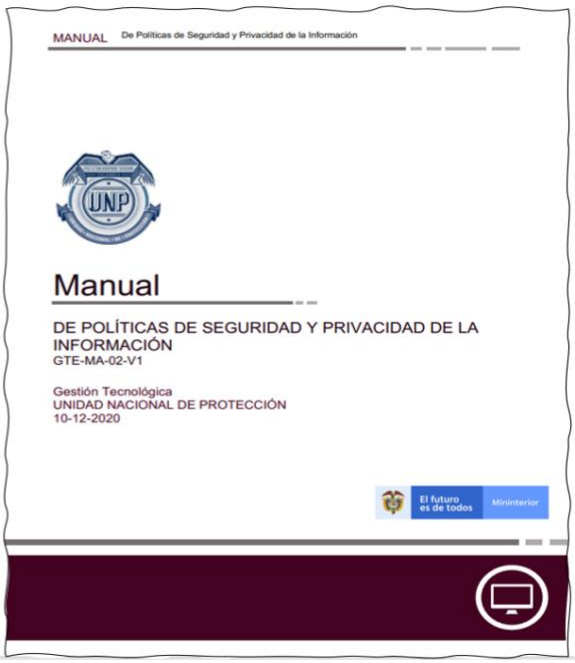
7 de junio se celebra el día mundial contra la falsificación y la piratería

30 de junio - Dia mundial de las redes sociales

Despliegue de la socialización del Manual de políticas específicas de seguridad y privacidad de la información.

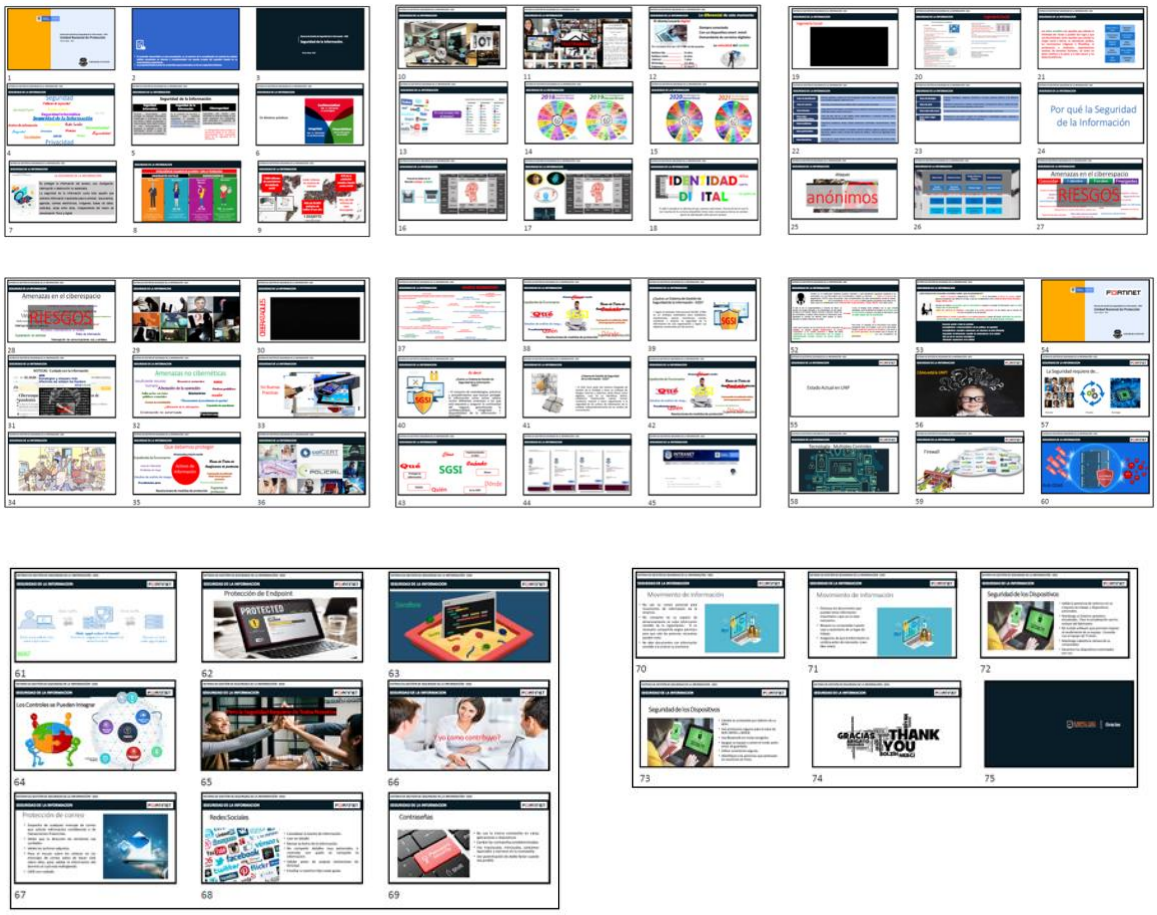
Socialización de las políticas de seguridad y privacidad de la información



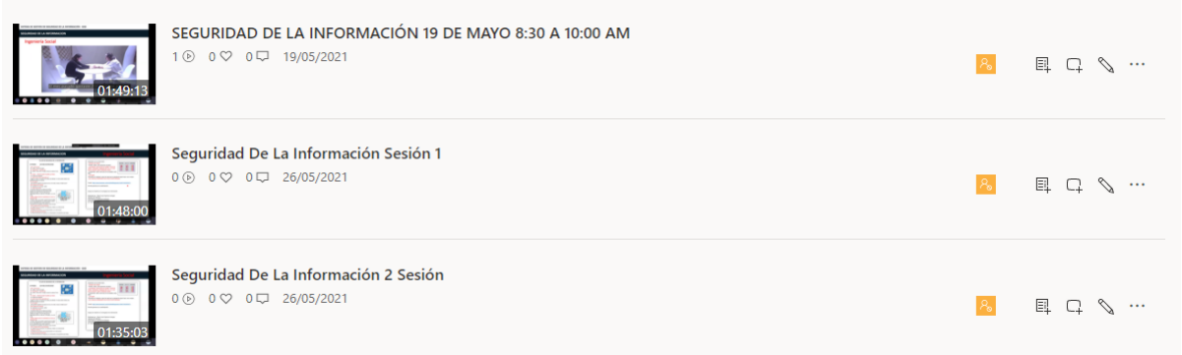


Charlas de seguridad de la información.

Charlas de Seguridad y privacidad de la información.

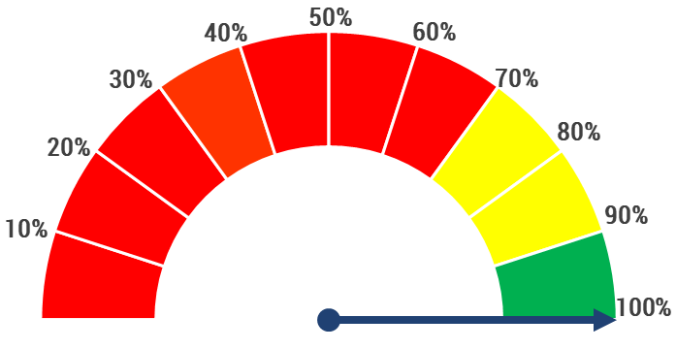


Sesiones grabadas



Objetivo: Definir y mantener actualizados los servicios de TI que permitan el cumplimiento de los objetivos estratégicos institucionales

Gráfico 4 Cumplimiento Objetivo 3 SGSI



Fuente: Elaboración Propia

El objetivo tuvo un cumplimiento promedio del **100%** donde el indicador evaluado en el período cumplió la meta planteada.

- **Actualización del Catálogo de servicios de TI**

Tabla 4 Actualización del catálogo de servicios T.I.

META	NOMBRE INDICADOR	FORMULA DE CÁLCULO	CUMPLIMIENTO	INDICADOR	Numerador del Indicador	Denominador del Indicador
100%	Actualización del Catálogo de servicios de TI	0% No tiene, 20% En implementación, 60% Implementado pero desactualizado, 100% Implementado y actualizado.	CUMPLE	100%	100	100

Fuente: Elaboración Propia

Actualización del Catálogo de servicios de TI

- Actualmente la Unidad Nacional de Proteccion- UNP cuenta con el documento oficial GTE-CT-01 V1 Catálogo de Servicios de Tecnologías de la Información.pdf, oficializado el día 30 de octubre del año 2020, este se encuentra en 100 % del indicador de eficacia en relación a entrega, así mismo se han venido elaborando actividades de actualización del documento paralelamente con estructuración del Acuerdo de Niveles de Servicio ANS, por lo cual se podría inferir que se han logrado avances de un 40 % para actualización a una nueva versión del documento.

GTE-SE-01	*Office 365 Herramienta ofimaticas*
GTE-SE-02	*Correo electronico*
GTE-SE-03	*Video conferencia*
GTE-SE-04	*Pandora - Sharepoint*
GTE-SE-05	*Biometricos*
GTE-SE-06	*System Center*
GTE-SE-07	*Gestion Usuarios*
GTE-SE-08	*Impresoras*
GTE-SE-09	*Botones de panico*
GTE-SE-10	*DHCP*
GTE-SE-11	*Sistemas de informacion - SER*
GTE-SE-12	*Sistemas de informacion - SOCRATES*
GTE-SE-13	*Sistemas de informacion - Formulario Web PQRS*
GTE-SE-14	*Sistemas de informacion - GEDOC*
GTE-SE-15	*Seguridad perimetral*
GTE-SE-16	*Directorio Activo*
GTE-SE-17	*Base de datos*
GTE-SE-18	*DNS*
GTE-SE-19	*Sistemas de informacion - TNS*
GTE-SE-20	*Sistemas de informacion - SIGOB*
GTE-SE-21	*Conectividad*
GTE-SE-22	*Portal WEB*
GTE-SE-23	*Internet*
GTE-SE-24	*Intranet*
GTE-SE-25	*UPS A/C Sistema electricos (FACILITIES)*
GTE-SE-26	*Telefonica*
GTE-SE-27	*Virtualización*
GTE-SE-28	*Azure*

CONCLUSIONES

- Es de anotar que este es un sistema de gestión nuevo para la entidad y actualmente se están adelantando actividades propias de la fase de planeación, la cual define los aspectos estratégicos que permiten en la fase del hacer, implementar los controles para posterior fase de verificación y mejora continua.

- Se vienen desarrollando actividades propias de la operación de la entidad, con controles administrativos, tecnológicos, operativos que se van a articular con la Declaración de aplicabilidad y el manual de políticas específicas de seguridad y privacidad de la información y que va a contribuir con el nivel de madurez del MSPI.