



**SEGUIMIENTO A LA POLITICA DEL SISTEMA DE GESTIÓN  
DE SEGURIDAD DE LA INFORMACIÓN**

**JUNIO 2021**

## SISTEMA DE GESTIÓN 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.

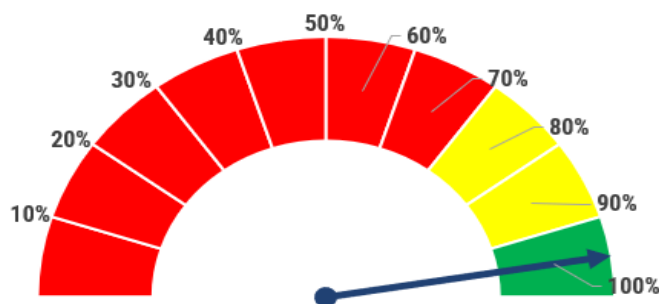
Los compromisos de seguridad de la información se despliegan a través de los siguientes objetivos:

- 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*

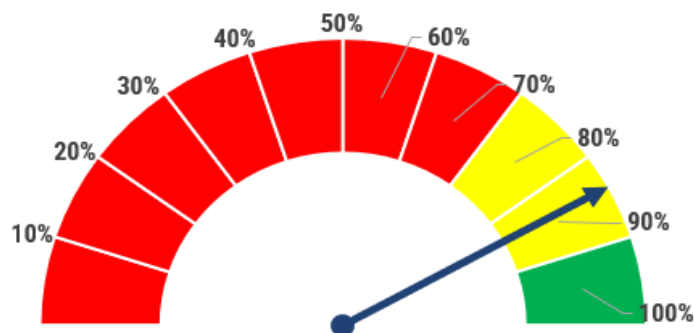
OBJETIVO MIPG-SIG	META	NOMBRE INDICADOR	CUMPLIMIENTO	INDICADOR
Implementar los controles del Modelo de Seguridad y Privacidad de la Información - MSPI a partir de los requisitos de seguridad con el propósito de gestionar los riesgos y preservar la confidencialidad, integridad y disponibilidad de los 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.

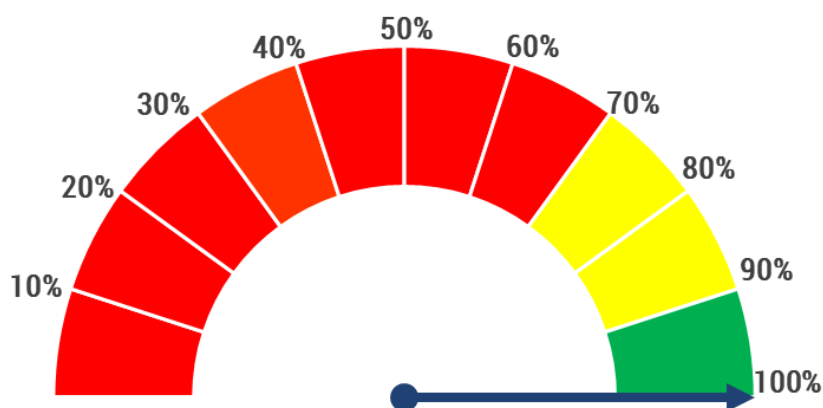
Los controles implementados se relacionan a continuación.

**UNIDAD NACIONAL DE PROTECCION**  
**DECLARACION 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	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	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 continúa.	SI	IMPLEMENTADO
A.6	Organización de la seguridad de la información	A.6.1	Organización interna	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	A.6.1.2	Separación de deberes.	Los deberes y áreas de responsabilidad en conflicto se deben separar para proteger la seguridad de la información de la información 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	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	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	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 étcas 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	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	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	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	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	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	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	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	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	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	A.11.1.1	Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usuarios 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	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	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	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	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	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	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	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	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	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	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 específicas 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

Resultados		Por Fecha
De	Asunto	Recibido
<b>La semana pasada</b>		
PONAL - CSIRT	NOTICIAS, TIPS Y ALERTAS CSIRT-PONAL	lunes 21/06/2021 5:34 p. m. 90 KB
NOTICIAS, TIPS Y ALERTAS CSIRT-PONAL Boletín Informativo No. 013 - Alerta de Malware circulando en la red Falso correo electrónico circulando a través de la red, informando sobre una retribución fiscal del presente año,		
PONAL - CSIRT	NOTICIAS, TIPS Y ALERTAS CSIRT-PONAL	domingo 20/06/2021 3:02 p. m. 90 KB
NOTICIAS, TIPS Y ALERTAS CSIRT-PONAL Boletín Informativo No. 012 - Alerta de Phishing circulando en la red Falso correo electrónico circulando a través de la red, informando sobre una suspensión de cuenta de		
<b>El mes pasado</b>		
PONAL - CSIRT	NOTICIAS, TIPS Y ALERTAS CSIRT-PONAL	lunes 31/05/2021 10:47 a. m. 97 KB
NOTICIAS, TIPS Y ALERTAS CSIRT-PONAL Boletín Informativo No. 011 - Alerta de Malware circulando en la red Falso correo electrónico circulando a través de la red, informando de una supuesta notificación realizada por parte		
PONAL - CSIRT	NOTICIAS, TIPS Y ALERTAS CSIRT-PONAL	viernes 14/05/2021 11:04 a. m. 97 KB
NOTICIAS, TIPS Y ALERTAS CSIRT-PONAL Boletín Informativo No. 010 - Alerta de Malware circulando en la red Se encuentra circulando a través de la red, mensaje falso sobre información de un supuesto envío realizado, y		
<b>Más antiguos</b>		
PONAL - CSIRT	NOTICIAS, TIPS Y ALERTAS CSIRT-PONAL	viernes 9/04/2021 1:01 p. m. 90 KB
NOTICIAS, TIPS Y ALERTAS CSIRT-PONAL Boletín Informativo No. 007 - Alerta de Phishing circulando en la red Informamos sobre campaña de spam a las cuentas de correos, usando una modalidad de extorsión con el fin de		

## Correos enviados al Webmaster para el diseño gráfico y posterior divulgación

**RV: Boletín Informativo – Alerta de Phishing circulando en la red.**

David Yacel Espinosa Vanegas  
Para: María Benavente Párraga

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

UNP-SGSI-BOLETIN-0004-Alerta Phishing circulando en la red - Estación Bli.com.docx

De: David Yacel Espinosa Vanegas  
Enviado: viernes, 9 de abril de 2021 3:43 p. m.  
Para: webmaster <webmaster@unp.gov.co>; Luis Alejandro Becerra Rojas <luis\_becerra@unp.gov.co>  
Asunto: Boletín Informativo – Alerta de Phishing circulando en la red.

Dándole cumplimiento al Plan de seguridad y privacidad de la información, dentro de las actividades a realizar se encuentra la difusión de las alertas de ciberseguridad publicadas por el CSIRT Ponal y/o el CCOCI (Comando Conjunto Cibernético) y otras fuentes autorizadas, por lo que requerimos de su acostumbrado apoyo para que se elabore la pieza gráfica respectiva para ser divulgada en toda la entidad.

La pieza informativa podría ser desplegada a través del correo electrónico y la intranet.

Elabore un modelo de plantilla para que vayamos revisando la posibilidad de generar un estándar y poder crear una libreta virtual con todas las boletines y alertas.

Adjunto la propuesta.

Cordialmente

David Yacel Espinosa Vanegas  
Contratista - CSISO - Oficial de Seguridad de la Información  
Grupo de Gestión de las Tecnologías de la Información - GGTI  
Oficina Asesora de Planeación e Información - OAPI  
david.espinosa@unp.gov.co  
Teléfono: 4269800 Ext. 9431

SENA NACIONAL DE PROTECCIÓN  
Carrera 83 # 14 - 87 / Primer Piso  
Puente Aranda / Bogotá D.C. Colombia  
PBX: (571) 4 26 98 00  
www.unp.gov.co

**RE: UNP-SGSI-BOLETIN-0003-Alerta Correo malicioso circulando en la red - suplantación DAFP**

David Yacel Espinosa Vanegas  
Para: webmaster

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

webmaster <webmaster@unp.gov.co>  
Enviado: jueves, 18 de abril de 2021 11:23 a. m.  
Para: David Yacel Espinosa Vanegas <david.espinosa@unp.gov.co>  
Asunto: RE: UNP-SGSI-BOLETIN-0003-Alerta Correo malicioso circulando en la red - suplantación DAFP

Asunto: correo suplanteo

Se anexa por la brevedad en la propuesta para haberse realizado una implementación en la página web por el tema de la norma y se da el tema prioritario, quedo atento a sus comentarios, saludos cordiales.

La Oficina Asesora de Planeación e Información a través del GGTI informa:

Que está circulando en las redes sociales un correo suplantando la Función Pública, en el cual se invita a un curso de actualización profesional, el cual se trata de un curso de actualización profesional, el cual se trata de un curso de actualización profesional.

Este correo contiene un enlace malicioso que busca extorsionar a los usuarios.

Alerta de seguridad

Estos enlaces pueden ser: Phishing, Malware o un falso correo electrónico, el cual se trata de un correo electrónico que busca extorsionar a los usuarios.

Consulte con sus superiores para que se elabore la pieza gráfica respectiva para ser divulgada en toda la entidad.

Adjunto la propuesta.

Cordialmente

David Yacel Espinosa Vanegas  
Contratista - CSISO - Oficial de Seguridad de la Información  
Grupo de Gestión de las Tecnologías de la Información - GGTI  
Oficina Asesora de Planeación e Información - OAPI  
david.espinosa@unp.gov.co  
Teléfono: 4269800 Ext. 9431

SENA NACIONAL DE PROTECCIÓN  
Carrera 83 # 14 - 87 / Primer Piso  
Puente Aranda / Bogotá D.C. Colombia  
PBX: (571) 4 26 98 00  
www.unp.gov.co

**Boletines Csirt Ponal - Alerta malware circulando en la red**

David Yacel Espinosa Vanegas  
Para: Luis Alejandro Becerra Rojas; webmaster  
CC: Francisca Rojas Montañez

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

UNP-SGSI-BOLETIN-0005-Alerta Malware circulando en la red - Cebalá Robledo.docx

UNP-SGSI-BOLETIN-0006-Alerta Malware circulando en la red - Panga Infal.docx

Dándole cumplimiento al Plan de seguridad y privacidad de la información, dentro de las actividades a realizar se encuentra la difusión de las alertas de ciberseguridad publicadas por el CSIRT Ponal y/o el CCOCI (Comando Conjunto Cibernético), por lo que requerimos de su acostumbrado apoyo para que se elabore la pieza gráfica respectiva para ser divulgada en toda la entidad.

La pieza informativa podría ser desplegada a través del correo electrónico y la intranet.

Adjunto los documentos con la propuesta:

Cordialmente

David Yacel Espinosa Vanegas  
Contratista - CSISO - Oficial de Seguridad de la Información  
Grupo de Gestión de las Tecnologías de la Información - GGTI  
Oficina Asesora de Planeación e Información - OAPI  
david.espinosa@unp.gov.co  
Teléfono: 4269800 Ext. 9431

SENA NACIONAL DE PROTECCIÓN  
Carrera 83 # 14 - 87 / Primer Piso  
Puente Aranda / Bogotá D.C. Colombia  
PBX: (571) 4 26 98 00  
www.unp.gov.co

**RE: NOTICIAS, TIPS Y ALERTAS CSIRT-PONAL**

David Yacel Espinosa Vanegas  
Para: webmaster

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

De: David Yacel Espinosa Vanegas <david.espinosa@unp.gov.co>  
Fecha: lunes, 31 de mayo de 2021, 11:23 a. m.  
Para: Luis Alejandro Becerra Rojas <luis\_becerra@unp.gov.co>; webmaster <webmaster@unp.gov.co>  
Asunto: RV: NOTICIAS, TIPS Y ALERTAS CSIRT-PONAL

Dándole cumplimiento al Plan de seguridad y privacidad de la información, dentro de las actividades a realizar se encuentra la difusión de las alertas de ciberseguridad publicadas por el CSIRT Ponal y/o el CCOCI (Comando Conjunto Cibernético), por lo que requerimos de su acostumbrado apoyo para que se elabore la pieza gráfica respectiva para ser divulgada en toda la entidad.

La pieza informativa podría ser desplegada a través del correo electrónico y la intranet.

Cordialmente

David Yacel Espinosa Vanegas  
Contratista - CSISO - Oficial de Seguridad de la Información  
Grupo de Gestión de las Tecnologías de la Información - GGTI  
Oficina Asesora de Planeación e Información - OAPI  
david.espinosa@unp.gov.co  
Teléfono: 4269800 Ext. 9431

SENA NACIONAL DE PROTECCIÓN  
Carrera 83 # 14 - 87 / Primer Piso  
Puente Aranda / Bogotá D.C. Colombia  
PBX: (571) 4 26 98 00  
www.unp.gov.co

Despliegue a toda la entidad.

**BOLETIN-UNP-SGSI**

Boletín Informativo CSIRT - PONAL No. 011  
**Alerta de Malware circulando en la red**

La Oficina Asesora de Planeación e Información a través del GTI, informa que esta circulando en la red:

Falso correo electrónico circulando a través de la red, informando de una supuesta notificación realizada por parte de la Fiscalía General de la Nación, la cual utiliza de remitente una cuenta de correo Hotmail (fiscaliageneralcuentadecobro4@hotmail.com) y cuenta con un archivo comprimido adjunto el cual contiene muestras maliciosas.

Absténgase de abrir y descargar este correo, elimínelo de la bandeja de entrada y de elementos eliminados. La descarga del archivo adjunto podría comprometer la información que se procesa sobre la infraestructura tecnológica de la UNP.

Este tipo de programas maliciosos puede afectar, no solo la información de la entidad, sino también la personal si se descarga desde los computadores o equipos móviles personales.

**RECOMENDACIONES**

- No ejecutar enlaces, archivos o imágenes recibidos desde correos no solicitados.
- No responda mensajes que le soliciten información personal o financiera.
- Eliminar los correos de remitentes desconocidos
- Mantener actualizados los sistemas operativos
- Mantener actualizado el antivirus.

Clic para más Información sobre este y otros boletines relacionados.

**BOLETIN-UNP-SGSI**

Boletín Informativo CSIRT - PONAL No. 012  
**Alerta de Malware circulando en la red**

La Oficina Asesora de Planeación e Información a través de GTE, informa que esta circulando en la red:

Falso correo electrónico circulando a través de la red, informando sobre una suspensión de cuenta de Outlook.com, este caso se trata de un Phishing, el cual busca obtener su datos personales, recuerden tener precaución con este tipo de mensajes, bloquear remitente y eliminar.

Absténgase de abrir y descargar este correo, elimínelo de la bandeja de entrada y de elementos eliminados. La descarga del archivo adjunto podría comprometer la información que se procesa sobre la infraestructura tecnológica de la UNP.

Este tipo de programas maliciosos puede afectar, no solo la información de la entidad, sino también la personal si se descarga desde los computadores o equipos móviles personales.

**RECOMENDACIONES**

Clic para más Información sobre este y otros boletines relacionados.

**BOLETIN-UNP-SGSI**

Boletín Informativo CSIRT - PONAL No. 010  
**Alerta de Malware circulando en la red**

La Oficina Asesora de Planeación e Información a través del GGTI, informa que esta circulando en la red:

Un mensaje falso sobre información de un supuesto envío realizado en donde le indican que para permitirle rastrear su paquete y volver a confirmar su dirección de entrega deben abrir un archivo adjunto al correo con el fin de ver los documentos de envío, el cual contiene muestras maliciosas que afectan la información de los equipos de cómputo.

Absténgase de abrir y descargar este correo, elimínelo de la bandeja de entrada y de elementos eliminados. La descarga del archivo adjunto podría comprometer la información que se procesa sobre la infraestructura tecnológica de la UNP.

Este tipo de programas maliciosos puede afectar, no solo la información de la entidad, sino también la personal si se descarga desde los computadores o equipos móviles personales.

**RECOMENDACIONES**

Clic para más Información sobre este y otros boletines relacionados.

**BOLETIN-UNP-SGSI**

Boletín Informativo CSIRT - PONAL No. 008  
**Alerta de Malware circulando en la red**

La Oficina Asesora de Planeación e Información a través del GGTI, informa que esta circulando en la red:

Una campaña de spam a las cuentas de correo, las cuales buscan engañar al ciudadano con una notificación falsa, donde supuestamente informan que su cedula de ciudadanía ha sido reportada como robada.

Absténgase de abrir y descargar este correo, elimínelo de la bandeja de entrada y de elementos eliminados. La descarga del archivo adjunto podría comprometer la información que se procesa sobre la infraestructura tecnológica de la UNP.

Este tipo de programas maliciosos puede afectar, no solo la información de la entidad, sino también la personal si se descarga desde los computadores o equipos móviles personales.

**RECOMENDACIONES**

Clic para más Información sobre este y otros boletines relacionados.

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

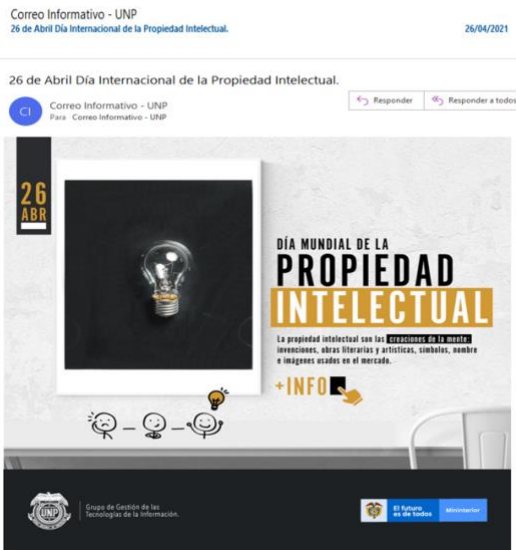
Se elaboraron los contenidos para el despliegue de los boletines relacionados con los siguientes días especiales.

✓ 26 de abril Día 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 - Día mundial de las redes sociales

## 26 de abril Día Internacional de la Propiedad Intelectual



## 6 de mayo se celebra el día internacional de la contraseña



# 17 de mayo - día internacional del internet

Correo Informativo - UNP  
 17 de mayo - Día Mundial del Internet  
 <http://intranet.unp.gov.co/DOCUMENTOS%20GGTI/DIA%20DEL%20INTERNET%20INFO.pdf> <fin>

17/05/2021

17 de mayo - Día Mundial del Internet

Correo Informativo - UNP  
 Para Correo Informativo - UNP

Responder Responder a todos Reenviar

lunes 17/05/2021 9:32 a. m.



## DÍA MUNDIAL DEL INTERNET

M A Y O 17

### ¿POR QUÉ SE CELEBRA EL DÍA MUNDIAL DE INTERNET?

Entre los objetivos de esta fecha se encuentra **acercar la tecnología a todos los quehaceres diarios de la ciudadanía.**

Internet se ha convertido en una herramienta indispensable para desarrollar diferentes tipos de actividades, facilitando procesos, tiempos de entrega de información e incluso facilitando el mismo acceso a contenido de entretenimiento.

"Es necesario contribuir a que se comience mejor Internet para que se convierta en un recurso mundial verdaderamente accesible al público. El 17 de mayo, se celebrará este día que servirá para dar a conocer este recurso mundial, ofreciendo las TIC a la sociedad y contribuyendo de diferentes formas a reducir la brecha digital", así quedó pactado en el Artículo 121 del documento de conclusiones de la Cumbre Mundial de la Sociedad de la Información, explicando la necesidad de internet en todas las esferas que componen la sociedad.

VENTAJAS	DESVENTAJAS
<ol style="list-style-type: none"> <li>1. Da información inmediata.</li> <li>2. Generaliza los contenidos.</li> <li>3. Elimina las barreras y el espacio.</li> <li>4. Facilita el acceso al aprendizaje.</li> <li>5. Permite el trabajo en línea.</li> <li>6. Aumenta la comunicación.</li> <li>7. Permite la globalización.</li> <li>8. Ofrece otras formas de entretenimiento.</li> <li>9. Crea nuevas empleos y formas de búsqueda.</li> <li>10. Nueva forma de gestionarnos.</li> </ol>	<ol style="list-style-type: none"> <li>1. Problemas de privacidad de la información.</li> <li>2. Poca veracidad de los contenidos.</li> <li>3. Amenazas como virus o spam.</li> <li>4. Creas adicciones.</li> <li>5. Inicia el sedentismo.</li> <li>6. Empobrece la comunicación familiar.</li> <li>7. Exposición a contenidos no deseados.</li> <li>8. Problemas para distinguir lo real de lo virtual.</li> </ol>

### BENEFICIOS DE INTERNET

Entre los beneficios que esta gran red de redes puede brindar a cualquier usuario se puede mencionar:

- Permite comunicación permanente entre usuarios ubicados en diferentes sitios geográficos a un bajo costo.
- Posibilita compartir y divulgar información a gran escala, fomentando la cooperación y colaboración entre un gran número de gremios de todo tipo (científicas, universidades, tecnológicas, etc).
- El Internet ha sido una herramienta fundamental para que las empresas puedan presentar y promocionar sus servicios y productos en forma masiva y extensiva a personas de todo el mundo.
- Gracias a Internet el conocimiento científico y tecnológico ha llegado casi en forma inmediata hasta las naciones subdesarrolladas y en vía de desarrollo en forma acelerada.

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

Correo Informativo - UNP  
 7 de junio- Día mundial contra la falsificación y la piratería  
 7/06/2021

7 de junio- Día mundial contra la falsificación y la piratería

Correo Informativo - UNP  
 Para Correo Informativo - UNP

Responder Responder a todos Reenviar

lunes 7/06/2021 11:23 a. m.



## DÍA MUNDIAL CONTRA LA FALSIFICACIÓN Y LA PIRATERÍA JUNIO 7

### ¿Por qué se celebra?

Este 7 de junio se conmemora el Día Mundial contra la Falsificación y Piratería, en el que se busca motivar a los usuarios para combatir en territorio y poner de manifiesto la necesidad de sensibilizar a la población sobre comprar en el mercado informal, haciendo especial énfasis en los productos que generan:

### ¿Que es la piratería?

El término piratería se da para referirse en materia de Propiedad Intelectual para referirse a las actividades ilegales de reproducción (copias) y distribución de programas de datos y producciones intelectuales. Estas actividades se generan sin obtener la debida autorización, identificación o en una infracción a derechos de autor o derechos conexos.

En particular, con esta actividad se pueden obtener obras y producciones intelectuales de distintos tipos tales como:

- Literatura
- Música
- Programas computacionales
- Programas de televisión
- Bases de datos que contribuyen creativos de carácter intelectual
- Programas de copiamiento de información (copia) o DVD.

### ¿Que es la falsificación?

El término falsificación se da para referirse en materia de Propiedad Intelectual, para referirse a las actividades ilegales de reproducción (copias) y distribución de programas de datos y producciones intelectuales. Estas actividades se generan sin obtener la debida autorización, identificación o en una infracción a derechos de autor o derechos conexos.

Entre los productos que pueden ser objeto de falsificación se cuentan:

- Ropa
- Medicinas y cosméticos
- Juguetes
- Cigarrillos
- Cables y artículos de lujo

### Diferencias

Diferencias clave entre la piratería y la falsificación de la Propiedad Intelectual:

1. La piratería es la copia y venta de un producto sin el consentimiento de su creador, mientras que la falsificación es el uso no autorizado de un producto para venderlo sin haberlo creado, sino como resultado del consentimiento de su creador y mucho más allá del consentimiento.
2. La piratería se identifica porque quienes la venden no esconden su condición de copias, ni el productor de origen original. El negocio radica en el consumo masivo y no en una respuesta económica, o lo cual quiere la falsificación.
3. La falsificación es la deliberada violación de un derecho de propiedad intelectual, entre los en nombre de una marca comercial, o se presenta en la deliberada intención en contra de un derecho de Propiedad Intelectual o Derechos de Autor.

## 30 de junio - Día mundial de las redes sociales

Correo Informativo - UNP  
30 Junio - Día mundial de las redes sociales. 9:03 a. m.

30 Junio - Día mundial de las redes sociales.

CI Correo Informativo - UNP  
Para Correo Informativo - UNP



**¿Por qué se celebra?**

El Día de las Redes Sociales es una celebración promovida por el blog de noticias de internet, Mashable. El propósito es que los usuarios participen en las diversas actividades que se ofrecen en el mundo, debatir y compartir experiencias e ideas con otros usuarios acerca del significado y sentido que tiene para ellos el social media, deliberando hacia donde van las tendencias de estos medios.

Peter Cashmore, fundador del sitio Mashable, decidió incentivar que los medios sociales o social media tengan un día en el calendario, fecha que sería propicia para charlas y eventos relacionados a anécdotas, incógnitas y experiencias en plataformas sociales y blogs, que hoy por hoy se convirtieron en una forma más de comunicación.

**Ventajas**

- Permiten crear comunidades para intercambiar comunicación e intereses comunes sobre todo tipo de temas.
- Pueden ayudar a tener más oportunidades profesionales, así como en la búsqueda de empleo.
- Facilitan las relaciones.
- Ayudan a que los más tímidos se relacionen con otros de forma más sencilla.
- Podemos estar informados en tiempo real de las noticias importantes y de todo lo que nos interesa.
- Permiten una comunicación instantánea.
- Ayudan con la formación, en modalidad a distancia o presencial.
- Mejoran un negocio.
- Tienen un poder viral.
- Pueden generar movimientos en masa de solidaridad en una situación de crisis.

**Desventajas**

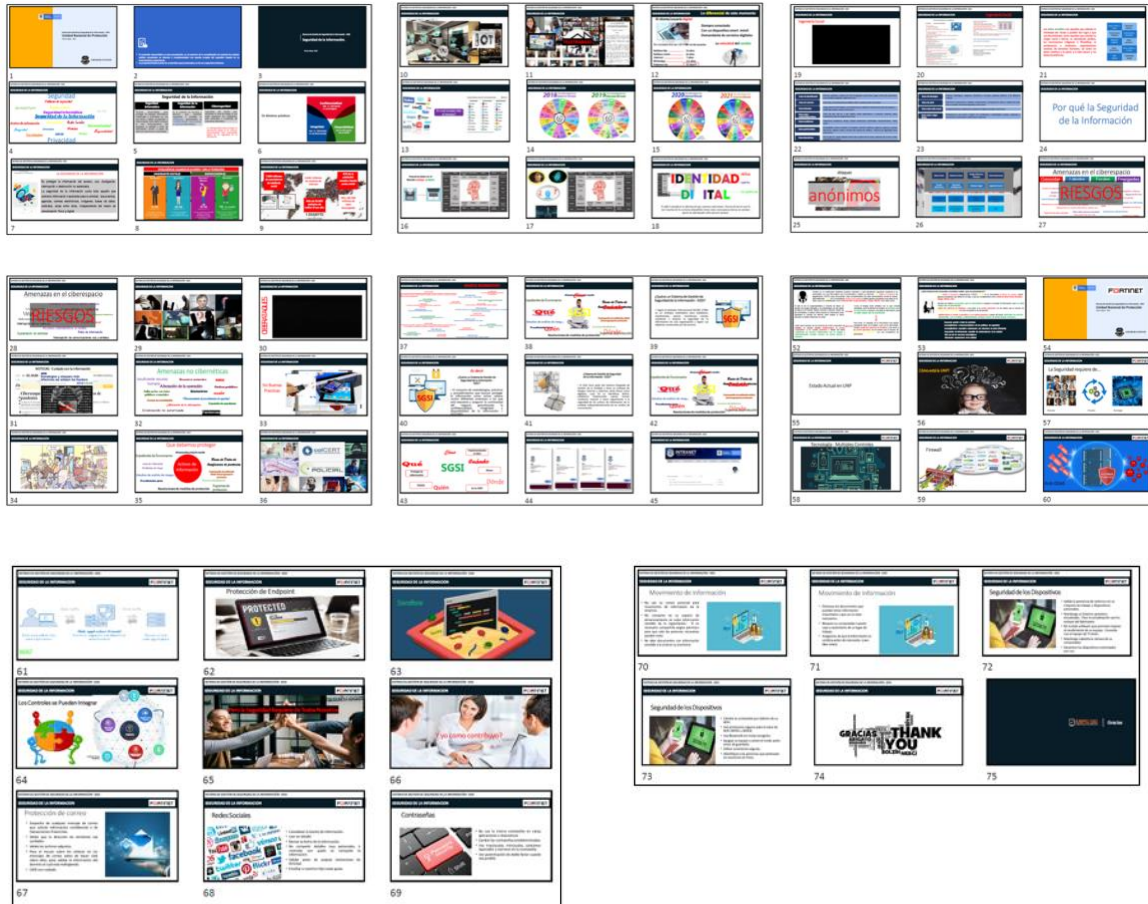
- Menos privacidad: se publica información personal que, en muchos casos, es vista por personas que no conocemos, perfumes y cosmeceúticos.
- Se pierde relación en el entorno físico (amigos y familiares), y la comunicación cara a cara disminuye.
- Pueden facilitar casos de ciberacoso, vulneración de la intimidad, suplantación de la identidad, robo de datos personales, etc.
- Es posible, en algunos casos, llegar a una ruptura de pareja debido a las redes sociales (por celos, control de la cuenta de la pareja, etc.).
- Informaciones falsas.
- Es muy sencillo mentir en las redes sociales, publicando solamente lo positivo y las cosas perfectas, dando una imagen de vida perfecta.
- Hacen perder el tiempo y perjudicar, en muchos casos, la productividad.
- Pueden perjudicar la imagen de un negocio.
- Pierden oportunidades laborales.

## 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.

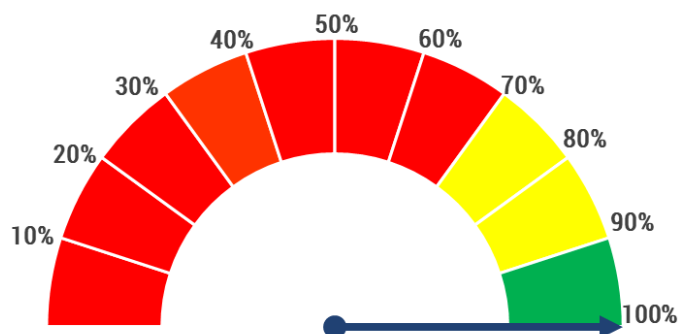


## Sesiones grabadas



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

## 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.