Guía del Plan de Comunicaciones para la Implementación del Sistema de Gestión de Seguridad de la Información en la SNR

SUPERINTENDENCIA
DE NOTARIADO Y REGISTRO

Código: SIG - SSI - PO - 04 - GI - 01	Versión: 01	Fecha: 06 de Diciembre de 2022

EQUIPO DIRECTIVO:

WILLIAM PEREZ CASTAÑEDA
SECRETARIA GENERAL
MARIO ALEXANDER ORTIZ SALGADO
JEFE OFICINA DE TECNOLOGIA DE LA INFORMACIÓN
JUAN CARLOS TORRES RODRÍGUEZ
COORDINADOR DEL GRUPO DE ARQUITECTURA ORGANIZACIONAL MEJORAMIENTO CONTINUO
LEYLA ZORAYA GUZMAN RODRIGUEZ
OFICINA DE TECNOLOGIA DE LA INFORMACIÓN
GRUPO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
OFICINA DE TECNOLOGIA DE LA INFORMACIÓN
GRUPO ARQUITECTURA ORGANIZACIONAL MEJORAMIENTO CONTINUO
OFICINA ASESORA DE PLANEACIÓN

República de Colombia

Ministerio de Justicia y del Derecho

Superintendencia de Notariado y Registro

TABLA DE CONTENIDO

1. INTRODUCCIÓN 4

2. MARCO LEGAL 4

3. OBJETIVO PLAN DE COMUNICACIONES 4

4. ENFOQUE DE LA ESTRATEGIA DE COMUNICACIONES. 5

4.1 DIRECCIONADORES GENERALES DE LA ESTRATEGIA DE COMUNICACIONES..... 5

4.2 FRENTES DEL PLAN DE COMUNICACIONES. 6

4.3 AUDIENCIAS CLAVE DEL PLAN DE COMUNICACIONES. 7

4.4 ENFOQUE PARA EL DISEÑO DE PIEZAS DE COMUNICACIÓN. 10

4.5 MATRIZ DE COMUNICACIONES. 11

4.5.1 Estructura de la matriz de Comunicaciones. 11

1. INTRODUCCIÓN

El presente documento tiene como fin presentar la estrategia de comunicaciones que se llevará a cabo para apalancar la implementación del Sistema de Gestión de Seguridad de la Información, en adelante SGSI en la SNR. El presente plan se ha desarrollado teniendo en cuenta los tiempos de implementación y pretende alinear a los equipos de trabajo y principales actores (partes interesadas) involucradas en su implementación. Se tendrá en cuenta para el despliegue de la estrategia el uso de piezas que deberán diseñarse con soporte del área de comunicaciones de la Entidad para ir cubriendo el soporte de conocimiento suficiente para que los actores claves puedan ser parte activa en la implementación del SGSI

2. MARCO LEGAL

Se formula en cumplimiento del mandato legal vigente del tema a tratar.

3. OBJETIVO PLAN DE COMUNICACIONES

Los principales objetivos para cubrir con esta estrategia y plan de comunicaciones para la implementación del SGSI son los siguientes:

1. Integrar un frente de comunicaciones generales de capacitación integral sobre el sistema de gestión de seguridad de la información. Estas comunicaciones pretenden capacitar en los conceptos clave a toso los funcionarios y Contratistas de la SNR. Las ideas centrales de este frente son:
    i. La Seguridad de la información es compromiso de todos
    ii. Los conceptos clave que debo conocer de la seguridad de la información.
2. Integrar un frente de comunicaciones preventivas, para promover en la comunidad general de la SNR valores asociados con la Seguridad de la información y direccionar acciones tendientes a su salvaguarda:
    i. Mi papel como funcionario y/o contratista de la SNR frente a la Seguridad de la información.
    ii. Las acciones que debo implementar para mejorar la seguridad de la información en la SNR.
3. Integrar un frente de comunicaciones de procedimientos a implementar, para comunicar roles y responsabilidades específicos en cada procedimiento a implementar y capacitar a los colaboradores de la SNR que participaran en la gestión del procedimiento. Asimismo, este frente cubre las comunicaciones para la implementación de I Solución:

i. El rol especifico y compromisos de los colaboradores de la SNR frente a la implementación del SGSI.
ii. Rol especifico y compromisos de los colaboradores usuarios de la plataforma I Solución.

4. Integrar un frente de comunicaciones de gestión orientadas a informar al Comité de Gestión y desempeño en el desarrollo del proyecto de implementación del SGSI.

4. ENFOQUE DE LA ESTRATEGIA DE COMUNICACIONES.

4.1 DIRECCIONADORES GENERALES DE LA ESTRATEGIA DE COMUNICACIONES.

Para el desarrollo del plan de comunicaciones se han tenido en cuenta los siguientes direccionadores generales.

i. El Rol del Comité de Gestión Institucional de la SNR como principal promotor en la implementación del SGSI y su compromiso con el éxito de la iniciativa.
ii. El Rol de los Coordinadores de Grupo de la SNR como pieza fundamental en la Gestión del Sistema de Gestión de seguridad de la información.
iii. El carácter de implementación masiva del SGSI en la SNR por su tamaño y múltiples ubicaciones debe considerar el aprovechamiento de herramientas propias de este tipo de implementación. Asimismo, debe contar con un líder por ubicación de la oficina que se encargue de la implementación del plan de comunicaciones y su seguimiento
iv. La estrategia de comunicaciones debe desarrollarse de manera paralela con el plan de implementación ya que uno de los objetivos es apalancar el cumplimiento del plan y hacer partícipe a toda la organización. En este sentido las herramientas y mecanismos utilizados deben permitir orientar información de carácter informativo y formativo a las audiencias clave y permitir al grupo SGSI evaluar su efectividad y aplicar mecanismos que promuevan su asimilación efectiva.
v. El desarrollo del plan se hará con fundamento en las comunicaciones registradas en la Matriz de Comunicaciones y el plan detallado a cubrir consignado en la Matriz de actividades detalladas que forman parte de esta Estrategia de Comunicaciones. Toda actualización a la Matriz de Comunicaciones debe tener en cuenta la actualización de la Matriz de actividades detalladas y gestionar los tiempos de la matriz de Actividades detalladas teniendo en cuenta la fecha de publicación estimada en la Matriz de Comunicaciones.
vi. El plan de comunicaciones considera el establecimiento de objetivos a partir de las necesidades identificadas de las partes interesadas. Las mas importantes se resumen en la sección **Audiencias Clave del plan de comunicaciones.**

4.2 FRENTES DEL PLAN DE COMUNICACIONES.

Para el desarrollo del plan de comunicaciones se han tenido en cuenta tres frentes a saber:

i. **Frente 1.** Comunicaciones informativas. Para el despliegue de las comunicaciones informativas con respecto al avance del proyecto e ir formalizando la base conceptual que debe formalizarse a la comunidad interna de la SNR (partes interesadas internas). Su objetivo principal es la capacitación con respecto a conceptos claves SGSI.

ii. **Frente 2.** Comunicaciones preventivas. Para el despliegue de las comunicaciones que orientan a las partes interesadas a prevenir eventos que puedan atentar contra la Integridad, privacidad y confidencialidad de la información. Su objetivo fundamental es la sensibilización.

iii. **Frente 3.** Comunicaciones asociadas a los procesos a implementar (Procesos SGSI). Consideran las comunicaciones que deben emitirse de acuerdo con el plan de implementación de los procedimientos del SGSI. Consideran tanto partes interesadas internas como externas que estén relacionadas con el procedimiento en implementación. Su objetivo fundamental es la capacitación/entrenamiento de las partes interesadas vinculadas a la ejecución del procedimiento.

Frente 3.1. Gestión de Activos de información. El objetivo de esta fase es identificar todos los activos de información relevantes (aquellos de calificación ALTA) que deben ser incluidos en la base de datos de Activos de información. Para esta fase el objetivo del plan es instruir y formar a los Coordinadores como actores clave de la fase.

Frente 3.2. Consolidación de la gestión de vulnerabilidades técnicas de Activos de Información SNR: En esta fase se debe formalizar el esquema de gestión de vulnerabilidades técnicas de los Activos de Información.

Frente 3.3. Gestión de incidentes de seguridad de la información. Durante la implementación se tendrá en cuenta partes interesadas tanto internas como externas que participan en el procedimiento. El frente debe tener en cuenta los medios que se utilizarán para dar a conocer a los ciudadanos y usuarios de los servicios de información los canales, formatos y procedimientos que se usarán para el reporte de incidentes de seguridad de la información.

Frente 3.4. Gestión de riesgos de seguridad de la información. El Grupo SGSI actuará como segunda línea de defensa soportando a la primera línea de defensa (Coordinadores de Grupo y

equipos de trabajo a cargo) en la identificación de directrices para la gestión de vulnerabilidades y amenazas asociadas a los Activos de información de los que son dueños/custodios y enfocados en aquellos de calificación ALTA. Los Coordinadores deben asegurar la identificación adecuada de vulnerabilidades y amenazas y la implementación de los controles para gestionar el riesgo inherente de los Activos de información y poder determinar su riesgo residual después de implementar los controles y de acuerdo con la metodología de Gestión de riesgos de seguridad de la información.

Frente 3.5. Implementación I Solución. Considera las comunicaciones básicas a tener en cuenta para la implementación de la plataforma I Solución.

4.3 AUDIENCIAS CLAVE DEL PLAN DE COMUNICACIONES.

Para el desarrollo de la estrategia se han identificado las siguientes audiencias clave:

i. Comité de Gestión Institucional / Comité de Seguridad de la Información (Parte Interna):

El Comité de Gestión Institucional que hace las veces de Comité de Seguridad de la Información es el emisor de las comunicaciones estratégicas en el proceso de implementación. Además, el Grupo SGSI debe mantenerlo informado sobre el avance de la estrategia. Estas comunicaciones estratégicas tienen por objeto dar fuerza a las decisiones y empoderar a los Coordinadores de Grupo de la SNR como actores clave en la implementación de la SNR.

En esta audiencia se involucra a la Secretaría General de la SNR y al área de comunicaciones de la SNR como ejecutor de las comunicaciones cuando sea necesario. Las necesidades específicas de esta parte interesada identificadas son:

1. Conocer aspectos relevantes de la implementación y asegurar su implementación efectiva.
2. Mantenerse informados sobre el avance en la implementación del SGSI de la SNR.
3. Motivar a las audiencias, especialmente las internas en la importancia de implementar el SGSI en la SNR.

ii. Coordinadores de Grupo de la SNR. (parte interna) Son los actores clave en la implementación del SGSI en la SNR.
Las necesidades de esta audiencia objetivo son las siguientes:

1. Empoderarlos efectivamente como Actores Clave en la implementación del SGSI. Su rol fundamental en la fase de Consolidación de la Base de datos de Activos de Información (su identificación, calificación, asignación de responsables y custodios y registrarlos en la base de datos SGSI) y durante la fase de Gestión de Riesgos (identificación de riesgos, vulnerabilidades y amenazas y la implementación de los controles para disminución del riesgo residual de los Activos de información a su cargo).
   Nota: Para el caso de los sitios de prestación de servicios registrales y notariales el Coordinador del Grupo dueño del proceso del nivel central debe nombrar formalmente un responsable por ubicación que lo represente en cada ubicación geográfica y que se encargue de gestionar las actividades asociadas con la implementación del SGSI.
2. Sensibilizarlos con respecto a los valores de la Seguridad de la información para que sean actores clave en la difusión a sus equipos de trabajo.
3. Capacitarlos en el manejo de los conceptos clave del SGSI como son:
   Frente 3.1. Consolidación de la Base de datos de Activos de Información:
   a. Saber identificar los Activos de Información.
   b. Saber cómo calificar los Activos de Información.

   Frente 3.2. Gestión de vulnerabilidades técnicas.
   a. Identificar controles para controlar las vulnerabilidades técnicas. (Grupos de trabajo encargados de resolverlas)
   b. Reconocer su rol en el aseguramiento de la implementación efectiva de los controles.

   Frente 3.3. Gestión de incidentes de seguridad de la información.
   a. Conocer los canales de reporte de incidentes de seguridad de la información.
   b. Consolidar la gestión de los grupos de trabajo que gestionaran los incidentes de seguridad de la información.
   Frente 3.4. Consolidación de la gestión de vulnerabilidades y amenazas a los Activos de Información.
   a. Saber identificar, calificar y valorar riesgos de seguridad de la información.
   b. Implementación de controles - Gestión del riesgo inherente y riego residual.

4. Soportarlos permanentemente en la solución de dudas e inquietudes durante la implementación.

iii. Comunidad interna.

Son todos aquellos funcionarios/contratistas con vinculación con la SNR y que forman parte de los Grupos de trabajo de la SNR. Las necesidades identificadas con esta audiencia son los siguientes:

1. Fomentar una cultura de Seguridad de la información.
2. Sensibilizar con respecto a el papel individual en la gestión de la Seguridad de la Información.
3. Sensibilizar con respecto al rol de dueño/custodio del AI.

iv. Comunidad externa de usuarios de servicio.

Son todas aquellas partes interesadas externas del SGSI que usan los servicios de la SNR. Audiencia constituida por personas naturales y jurídicas que usan los servicios de la SNR tanto públicas como privadas. Los objetivos específicos con esta parte interesada son:

1. Sensibilizarlos con respecto a su rol activo en los procedimientos de seguridad de la información de la SNR.
2. Identificar los canales de atención de solicitudes referentes a la Seguridad de la Información (canales a usar: línea 8000 y/o e-mail y/o portales).
3. Motivarlos a comunicar aspectos relevantes con la seguridad de la información de la Entidad.

v. Comunidad Interna de Control.

Constituida por los entes internos de control como Control Interno, Oficial de Seguridad de la información, Comité de Gestión Institucional y otros establecidos para el control del Sistema de Seguridad de la Información de la SNR.
Las necesidades con esta parte interesada son:

1. Mantenerlos informados con respecto a la implementación del SGSI y obtener su retroalimentación.
2. Aclarar su rol frente al SGSI en la SNR.

vi. Comunidad externa de Control.

Constituida por las Entidades externas y entes de control que regulan o supervisan la gestión del Sistema de Seguridad de la Información. DAFP, MINTIC, etc.
Los objetivos con esta audiencia:

1. Informar sobre requerimientos específicos a cumplir con entes de control durante la implementación y de acuerdo con el marco normativo vigente.

Nota: las comunicaciones a implementar con la Comunidad externa se irán implementando en la medida del avance de la implementación. Solo se establecen aquellas que han sido producto del análisis de las guías MSPI tenidas en cuenta hasta el momento.

4.4 ENFOQUE PARA EL DISEÑO DE PIEZAS DE COMUNICACIÓN.

Se usara formato único de comunicaciones basados en tres apartes, una pieza central que contiene la idea fuerza y un resumen y dos links, el primero a una pieza de profundización de conocimiento y un segundo link a una pieza de acciones que se deben implementar.
El ejemplo para la primera pieza del plan de comunicaciones se muestra a continuación:

La secuencia de despliegue la marca la pieza inicial (Parte superior) y al indicar el link de conocimiento se despliega la pieza inferior izquierda y para el link de acciones se desplegará la pieza en la parte inferior derecha. Para el caso de una pieza de comunicaciones preventivas el ejemplo se muestra a continuación.

Dado que el esquema de comunicaciones será exigente en su producción, es preciso validar su gestión directa por el grupo SGSI con esquema en el cual podamos actualizar los textos e imágenes de las piezas en una herramienta que nos suministre el área de comunicaciones de la Entidad.

4.5 MATRIZ DE COMUNICACIONES.

Para hacer seguimiento al plan de comunicaciones durante su implementación se anexa tabla al presente informe denominada Matriz de Comunicaciones SGSI.

4.5.1 Estructura de la matriz de Comunicaciones.

La Matriz de Comunicaciones está conformada por los siguientes campos:

1. Secuencia. Indica el número de consecutivo de la comunicación.

2. Nombre de la comunicación. Se identifica el nombre general de la comunicación.

3. Objetivo de la comunicación. Se identifica el objetivo principal de la comunicación. Este objetivo debe definir de manera clara y precisa lo que se pretende con la comunicación de acuerdo con la audiencia objetivo.

4. Frente de trabajo. Se especifica el frente de trabajo del plan de comunicaciones (Frente 1. Comunicaciones informativas, Frente 2 Comunicaciones preventivas, Frente 3. Comunicaciones por procedimiento a implementar + nombre del procedimiento).

5. Tipo de Comunicación. Se identifica el tipo de Comunicación. Este tipo de comunicación lleva implícito el canal que se va utilizar y por esta razón también asocia el mecanismo de evaluación de efectividad de la comunicación como se define a continuación. Entre los tipos de comunicación se tendrán en cuenta:
    - Campaña e-mail
    - Protector de pantalla (screensavers)
    - Medio publicitario en sitio
    - Medio publicitario masivo externo
    - Video institucional.
    - Capacitación virtual.
    - Medios implementación proyecto (carpetas compartidas, estrategia preguntas frecuentes, publicación guías y capacitación en línea).

6. Audiencia Objetivo. Se especifica uno de los tipos de Audiencia identificados en la sección **Audiencias Clave del plan de comunicaciones en la implementación del SGSI y objetivos específicos**. Determina la Audiencia objetivo de la comunicación y de manera implícita se establece el canal y el mecanismo para determinar su efectividad por el tipo de Comunicación considerado en el campo Tipo de Comunicación.

7. Detalle Audiencia objetivo. Se indica si se trata de un subconjunto de la Audiencia Objetivo definida.

8. Emisor de la comunicación. Se identifica de manera clara y concisa el ente emisor de la comunicación. Como entes formales Emisores de comunicaciones se establecen:
    - Comité de Gestión y desempeño Institucional.
    - Oficial de Seguridad de la Información.

- Jefe de Oficina (de Tecnologías de la Información, Control Interno, Planeación, Área misional, Secretaria, etc.). Siempre que se establezca como emisor el jefe de oficina debe especificarse el nombre del Área funcional.
- Mesa de trabajo SGSI.

9. Detalle del emisor. Se especifica en detalle el Emisor. Por ejemplo si en 8 se definió Jefe de Oficina en esta columna se coloca la oficina especifica (OTI, OAP,etc).

10. Ente Aprobador: es el nombre del ente que debe aprobar la comunicación antes de su emisión.

11. Líder de gestión de la comunicación. Identifica al miembro del grupo SGSI encargado de gestionar la comunicación.

12. Fecha proyectada. Identifica la fecha en formato aaaa/mm/dd en que se espera emitir la comunicación.

13. Estado de ejecución. Especifica uno de tres estados: Pendiente, Aplazada, Emitida. 4. ANEXOS Matriz de comunicaciones.

5. GLOSARIO DE TÉRMINOS

Activo: Recurso del sistema de información o cualquier elemento que tenga valor para la organización, hacen parte de los activos de información los siguientes:

Activo de Información: Todo aquel elemento lógico o físico que conforme cualquiera de los sistemas de información y que tiene un valor para la institución. Ej. Bases de datos, sistemas operacionales, redes, sistemas de información y comunicaciones, documentos impresos, fichas, formularios y recursos humanos.

Confidencialidad: Característica de la información por medio de la cual no se revela ni se encuentra a disposición de individuos, organizaciones o procesos no autorizados. La información debe ser vista o estar disponible solo a las personas autorizadas.

Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la Superintendencia de Notariado y Registro. Ejemplo: archivo de Word ¨listado de personal.docx¨.

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Correo electrónico: También conocido como E-mail, es un servicio de red que permite a los usuarios enviar y recibir textos, imágenes, videos, audio, programas, a través de internet.

Incidente: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Incidente de Seguridad de la información: Es la identificación de la ocurrencia de un hecho que está relacionado con los activos de información, que indica una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

Sistema de Gestión de Seguridad de la información: SGSI La parte del sistema total de gestión, basada en un enfoque de riesgo de negocios, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Seguridad: Mecanismos de control que evitan el uso no autorizado de recursos, no es un producto sino un proceso, en el que intervienen todos los aspectos de la tecnología y también las personas, siendo estas últimas por lo general el eslabón más débil de toda la cadena.

Seguridad de la Información: Son medidas preventivas que incluyen factores de confidencialidad, integridad, disponibilidad, autenticidad, responsabilidad, aceptabilidad y confiabilidad de la información e incluye aquellos aspectos sistémicos de la gestión de la seguridad, como podrían ser: Gestión de la seguridad de la información, asesoría y auditoría de la seguridad, análisis y gestión de riesgos, continuidad de negocio, gobierno, comercio electrónico y legislación relacionada con seguridad.

Definido también en el artículo 2.2.9.1.1.3 del Decreto 1078 de 2015 como el principio que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Seguridad informática: Aspectos de seguridad que inciden o tienen que ver directamente con la informática; es decir, en los medios informáticos en los que se genera, gestiona, almacena o destruye esta información, pero sin profundizar en aspectos sistémicos de la gestión de esa seguridad.

6. BIBLIOGRAFÍA

- Ministerio de Tecnologías de la Información y las Comunicaciones, Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información, articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf (mintic.gov.co),2022

7. ANEXOS

Matriz de plan de comunicaciones

VERSIÓN DE CAMBIOS			
Código:	**Versión:**	**Fecha:**	**Motivo de la actualización:**

ELABORACIÓN Y APROBACIÓN					
ELABORÓ	**REVISIÓN METODOLOGICA**	**APROBÓ**		**Vo.Bo Oficina Asesora de Planeación**	
Jaime Enrique Camacho Pardo Jorge Alberto Echeverri	Jeiffe Jubelly Muñoz Robayo	Leyla Zoraya Guzmán Rodríguez	Oficina de Tecnología de la Información	Juan Carlos Torres Rodríguez	Coordinador del Grupo de Arquitectura Organizacional Mejoramiento Continuo **o quien haga sus veces**
Oficina de Tecnología de la Información – Sistema de Gestión de Seguridad y Privacidad de la información	Oficina Asesora de Planeación.				
Fecha: 03 de Noviembre de 2022	Fecha: 29 de Noviembre de 2022	Fecha: 30 de Noviembre de 2022		Fecha Aprobación: **06 de Diciembre de 2022**	