UNGRD
Unidad Nacional para la Gestión del Riesgo de Desastres

Sistema Nacional de Gestión del Riesgo de Desastres

Sistema Integrado de Planeación y Gestión de la UNGRD certificado en:

ISO 9001:2015 ISO 14001:2015 OHSAS 18001:2007

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

21 // 01 // 2019

Oficina Asesora de Planeación e Información //

El futuro es de todos

Presidencia de la República

UNGRD
Unidad Nacional para la Gestión del Riesgo de Desastres
Sistema Nacional de Gestión del Riesgo de Desastres

Formato de documento

Título:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información				
Fecha de Aprobación:	25/01/2019				
Palabras claves:	Seguridad de la Información, tecnología , información, comunicaciones, infraestructura, aplicaciones, marco de referencia, arquitectura empresarial, PETI, UNGRD				
Formato:	PDF	**Lenguaje:**	Español		
Dependencia:	Oficina Asesora de Planeación e Información				
Código:		**Versión:**	1.0	**Estado:**	
Categoría:	Planes				
Autor(es):	Carolina Jiménez Zapata Luz Paula Contreras Murcia				
Revisó:	Luz Paula Contreras Murcia Javier Edgardo Soto Argel Luis Javier Barrera Naicipa				
Aprobó:	Juan José Neira Santacruz				
Ubicación:	Oficina Asesora de Planeación e Información				

Contenido

1.Objetivo

Detallar el plan de tratamiento de riesgos que hace parte del Sistema de Gestión de Seguridad de la Información – SGSI de la Unidad Nacional para la Gestión del Riesgo de Desastres, mediante el cual se definan los controles que permitan mitigar la materialización de los riesgos de seguridad de la información en la UNGRD.

2.Alcance

El plan de tratamiento de riesgos tiene alcance para el proceso de Gestión de Sistemas de Información y el subproceso de Infraestructura Tecnológica de la UNGRD, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información[1].

3.Términos y Definiciones

Riesgo: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

Seguridad de la Información: Este principio 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.

4.Planes Desarrollados de Riesgos de Seguridad y Privacidad de la Información

Para la vigencia 2018, el plan de tratamiento de riesgos contemplaba cuatro actividades correspondientes a:

	Actividad	Responsable	Fecha Inicial	Fecha Final
1	Realizar la evaluación de vulnerabilidad y Ethical Hacking sobre los sistemas de información de la entidad.	Infraestructura Tecnológica	01/06/2018	20/09/2018
2	Implementar el sistema de Seguridad Perimetral (fortalecimiento de infraestructura de seguridad para los sistemas de información, detección y tratamientos de día cero)	Infraestructura Tecnológica	01/06/2018	30/12/2018
3	Hacer seguimiento a la ejecución del Ethical Hacking y a la implementación de la Seguridad Perimetral en la entidad	Sistemas de Información	31/10/2018	30/12/2018
4	Elaborar el plan de mitigación de vulnerabilidades	Infraestructura Tecnológica/ Sistemas de Información	01/11/2018	30/12/2018

5.Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

En el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información –SGSI de la Unidad Nacional para la Gestión del Riesgo de Desastres, se busca prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad de la información, por lo cual es importante controlar y establecer los riesgos de seguridad de la información.

5.1 Planes Desarrollados de Seguridad y Privacidad de la Información.

Para el año 2018 se tenían planeadas dos actividades, las cuales correspondían a la implementación de una siguiente fase del SGSI que abarcara todos los procesos de la UNGRD, y actividades de Sensibilización de Seguridad de la Información.

La primera de dichas actividades estaba directamente relacionada con la consecución de recursos para la misma, los cuales no fueron asignados en la vigencia para su desarrollo.

Las actividades de sensibilización tal como se encontraban programadas en el plan, fueron realizadas, una por semestre, en el marco de los ejercicios de inducción y reinducción del personal de la UNGRD.

5.2 Riesgos de Seguridad y Privacidad de la Información.

A continuación se muestran los riesgos de Seguridad de la Información que se encuentran clasificados como en Zona de Riesgo Extrema, los cuales se encuentran asociados al Sistema de Gestión de Seguridad de la Información – SGSI de la Unidad Nacional para la Gestión del Riesgo de Desastres.

	Activo de Información	Riesgo	Plan de Tratamiento	Descripción
1	Switch	Configuración inadecuada	Reducir el riesgo, evitar, compartir o transferir	Se sugiere incluir dentro de los estudios previos para la adquisición del hardware asociado la capacitación a los funcionarios de la UNGRD sobre la configuración de los mismos. Además sugiere solicitar los manuales de configuración de los equipos.
2	Servidores físicos	Configuración inadecuada	Reducir el riesgo, evitar, compartir o transferir	Se sugiere incluir dentro de los estudios previos para la adquisición del hardware asociado la capacitación a los funcionarios de la UNGRD sobre la configuración de los mismos. Además sugiere solicitar los manuales de configuración de los equipos.
3	Servidores virtuales (HYPER -V)	Utilización errada o inadecuada	Reducir el riesgo, evitar, compartir o transferir	Se sugiere establecer un procedimiento de monitoreo adicional, para determinar si el uso previsto del servidor virtual está dentro de lo que se requiere. Así mismo el monitoreo debería incluir la planificación de la capacidad del servidor, identificación y corrección de problemas de Hiper V, así como la adecuación del tamaño de la máquina virtual.
4	Motor de base de datos (SQL Server)	Acceso no autorizado	Reducir el riesgo, evitar, compartir o transferir	Se sugiere robustecer las contraseñas de acceso de acuerdo a la política de control de acceso definida para la entidad.
5	Motor de base de datos (Postgres)	Acceso no autorizado	Reducir el riesgo, evitar, compartir o transferir	Se sugiere robustecer las contraseñas de acceso de acuerdo a la política de control de acceso definida para la entidad.
6	Firewall Untangle	Daño (pérdida parcial)	Reducir el riesgo, evitar, compartir o transferir	Se sugiere contar con un proveedor de hardware que reponga alguna parte específica o el HW en su totalidad con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la

				información.
7	Impresoras	Robo de documentos o información	Reducir el riesgo, evitar, compartir o transferir	Se sugiere realizar una sensibilización sobre la utilización y manejo de los documentos impresos por parte de los funcionarios y contratistas de la Entidad.
8	Scanners	Robo de documentos o información	Reducir el riesgo, evitar, compartir o transferir	Se sugiere realizar una sensibilización sobre la utilización y manejo de los documentos escaneados por parte de los funcionarios y contratistas de la Entidad.
9	Plotter	Robo de documentos o información	Reducir el riesgo, evitar, compartir o transferir	Se sugiere realizar una sensibilización sobre la utilización y manejo de los documentos impresos por parte de los funcionarios y contratistas de la Entidad.

5.3 Actividades a Desarrollar sobre los Riesgos de Seguridad y Privacidad de la Información.

	Actividad	Descripción	Responsable	Fecha Inicial Planificada	Fecha Final
1	Diagnóstico del SGSI frente a la 27001	Realizar la revisión de los procesos vinculados al actual SGSI, a la luz de la ISO 27001, y sus respectivos mapas de riesgo del SGSI	Paula Contreras Carolina Jiménez Luis Javier Barrera Javier Soto	04/02/2019	18/02/2019
2	Programación y ejecución de Campañas de Uso y Apropiación del SGSI	Definir y ejecutar las actividades en el marco de las campañas de uso y apropiación de las TIC, enfocadas en el SGSI.	Paula Contreras Carolina Jiménez Luis Javier Barrera Javier Soto	18/02/2019	31/12/2019
3	Verificación e implementación de indicadores de SGSI	Identificar los indicadores recomendados para el SGSI, verificar cuáles ya se encuentran implementados y definir los que se van a implementar	Paula Contreras Carolina Jiménez Luis Javier Barrera Javier Soto	25/02/2019	01/03/2019
4	Elaboración del Plan de mitigación de vulnerabilidades	Basados en el informe del Ethical Hacking desarrollado en la entidad, se elaborará el Plan de Mitigación de Vulnerabilidades identificadas	Paula Contreras Carolina Jiménez Luis Javier Barrera Javier Soto	25/02/2019	01/04/2019

5.4 Programación de Monitoreo de Controles de Riesgos de Seguridad y Privacidad de la Información.

Teniendo en cuenta que el Sistema de Gestión de Seguridad de la Información – SGSI hace parte del Sistema Integrado de Planeación y Gestión – SIPLAG, el monitoreo de controles se realizará con la misma periodicidad con la que se realiza la revisión de los mapas de riesgo por proceso, esto es, de forma cuatrimestral.

6.Marco Legal

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de Abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de Junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

7.Documentos Asociados

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
- M-1603-SIS-04 Manual del Sistema de Gestión de Seguridad de la Información.
- M-1603-SIS-03_3 Manual de Políticas de Seguridad de la Información.
- RG-1603-SIS-17 Formato Matriz de Riesgos SGSI UNGRD Infraestructura.
- RG-1300-GSI-12 Formato Matriz de Riesgos SGSI UNGRD Aplicaciones.