PLAN DE TRATAMIENTO DE RIESGOS

Noviembre de 2017

	NOMBRE	CARGO	FECHA
ELABORÓ	Néstor Julio Corredor	Profesional Especializado	11/2017
REVISÓ	Néstor Julio Corredor	Profesional Especializado	11/2017
APROBÓ	Cesar Augusto Rincón Vicentes	Director Administrativo y Financiero	30/11/2017

CONTENIDO

INTRODUCCION

Este documento presenta la guía para encontrar dentro de Global Suite el Plan de Tratamiento recomendado para los riesgos de seguridad de la información identificados en el CNMH. El plan de tratamiento de riesgos representa el mejoramiento continuo del SGSI y el propuesto para el CNMH se basa en la norma NTC-ISO/IEC 27001:2013.

En el anexo A de la norma NTC-ISO/IEC 27001:2013 se establecen 114 controles distribuidos en 14 dominios que presentan las mejores prácticas para el tratamiento de los riesgos contra la confidencialidad, integridad y disponibilidad de la información.

1. ASPECTOS GENERALES

1.1. OBJETIVO

Presentar el Plan a ser ejecutado para el tratamiento de los riesgos de seguridad de la información que se encuentran por fuera del Nivel de Riesgo Aceptable NRA por parte del CNMH.

1.2. ALCANCE

Este inventario fue desarrollado para los procesos del alcance del SGSI y son los siguientes:

- Difusión de Memoria Histórica
- Acuerdos de la Verdad
- Investigaciones
- Registro y Acopio
- Procesamiento
- Talento Humano
- Gestión de las TIC

2. DEFINICIONES

Activo: Cualquier elemento que tiene valor para la organización y que para la gestión de riesgos de seguridad de la información se consideran los siguientes tales como: la información, el software, elementos físicos, los servicios, las personas e intangibles.

Amenaza: Causa potencial de un incidente no deseado, el cual puede resultar en daño al sistema o a la Organización.

[Fuente: ISO 27000]

Confidencialidad: Propiedad de la información que hace que no este disponible o que sea revelada a individuos no autorizados, entidades o procesos.

Disponibilidad: Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada.

[Fuente: ISO 27000]

Importancia del activo: Valor que refleja el nivel de protección requerido por un activo de información frente a las tres propiedades de la seguridad de la informacion: integridad, confidencialidad y disponibilidad.

Integridad: Propiedad de precisión y completitud.

[Fuente: ISO 27000]

Monitoreo: Verificación, supervisión, observación crítica o determinación continua del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

Parte involucrada: Persona u organización que puede afectar, verse afectada o percibirse así misma como afectada por una decisión o una actividad. Una persona que toma decisiones puede ser una parte involucrada.

[Fuente: ISO 31000]

Propietario del activo: Persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El propietario del activo aprueba el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.

Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización)

[Fuente: ISO 31000]

- **Vulnerabilidad:** Debilidad identificada sobre un activo que puede ser aprovechada por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información

2. PLAN DE TRATAMIENTO

2.1. METODOLOGÍA

Presentar el Plan a ser ejecutado para el tratamiento de los riesgos de seguridad de la información que se encuentran por fuera del Nivel de Riesgo Aceptable NRA por parte del CNMH.

El Plan de Tratamiento hace parte de la aplicación de la Metodología de Gestión de Riesgos acogida por el CNMH y que se encuentra descrita en el documento Metodología de Gestión de Riesgos. El tratamiento se aplica para aquellos riesgos que por no encontrarse en el Nivel de riesgo Aceptable NRA, se debe reducir su probabilidad de ocurrencia y/o su impacto y para esto se aplica el control seleccionado con base en el Anexo A de la Norma NTC-ISO/IEC 27001:2013.

El Plan de tratamiento corresponde a los riesgos identificados sobre un grupo de activos clasificados como se muestra en la Tabla 1.

N.	Tipo de activo	Cantidad
1	Información	88
2	Software	18
3	Hardware	11
4	Personas	5
5	Instalaciones	2
6	Procesos	1
7	Redes de Comunicaciones	1
TOTAL		126

Tabla 1 – Activos cubiertos en el Plan de Tratamiento

Para estos 126 activos fueron detectados 846 riesgos de los cuales 490 no superan el NRA y deben ser tratados tal como se puede evidenciar en Global Suite como se muestra en la Figura 1.

Figura 1 Riesgos que deben ser tratados

2.2. CONTROLES

La definición de los controles para el Plan de Tratamiento se configuró en Global Suite considerando el estado actual, es decir el correspondiente al riesgo residual por encima del Nivel de Riesgo Aceptable NRA. Se tomó como guía los Controles propuestos en el Anexo A de la norma ISO 27001:2013, los cuales fueron registrados en Global Suite en la sección de Catálogos de Riesgos, la cual se accede a través de las siguientes Opciones:

- Dentro del menú principal se escoge la opción Administración
- Una vez en la parte de administración dentro de la opción de Plantillas, seleccionar la opción Catálogos de Análisis
- Dentro de la opción de Catálogos de Análisis seleccionar la opción Catálogos Riesgos Seguridad de la Información
- Siguiendo los pasos anteriores se llega a la sección donde se encuentran las ventanas del Catálogo, Amenazas y Controles.
- En la ventana de Controles se configuran los controles correspondientes al Anexo A de la ISO 27001 tal como se describió anteriormente.
- El paso final es la asociación de los controles con las amenazas del Catálogo que corresponde al tratamiento que se aplicaría en caso de que el riesgo identificado este por encima del NRA. Esto se visualiza en la figura 2

Figura 2. Controles asociados a las amenazas.

En la pantalla mostrada en la figura 2, se muestra en el panel izquierdo el tipo de Activo, que para este caso es Comunicaciones y en seguida las amenazas, que en este caso empiezan por Acceso no autorizado y luego se despliegan los controles sugeridos que podrían aplicar para los riesgos generados. Aplicando este enfoque se logra utilizar la herramienta Global Suite para la gestión SGSI del CNMH, en concordancia con los requisitos establecidos en la norma ISO 27001:2013.

Una vez cumplido con el paso anterior de definición de los controles y asociación con las amenazas del Catálogo, se procede con la definición del plan de Tratamiento y que se cumple con los siguientes pasos:

- Dentro del menú principal de Global Suite, se escoge la opción **Análisis**
- En el menú dentro de la opción Análisis, en la sección de Opciones se selecciona **Gestión de riesgos**
- Posteriormente se debe seleccionar **Análisis de CENTRO NACIONAL DE MEMORIA HISTÓRICA**
- Esto despliega una pantalla dividida en 2 secciones, tal como se muestra en la figura 3, en donde en la parte superior se encuentran los activos de información con las amenazas identificadas en la fase de Análisis de Riesgos y en la parte inferior los controles que se habían implementado en el Catálogo de amenazas como se describió anteriormente.

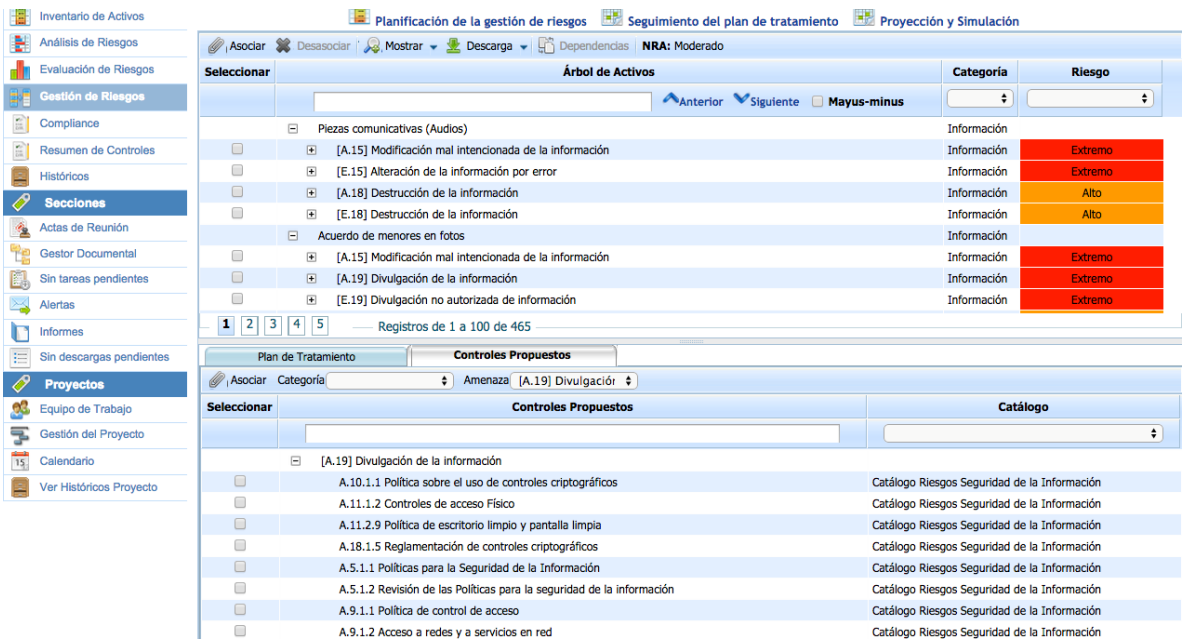

Figura 3. Asociación de controles

- El siguiente paso es la definición del Plan de tratamiento, que se hace verificando cuales son las amenazas que generan riesgos que están por encima del NRA, que para el caso del CNMH, corresponden a los riesgos calificados en los niveles de Alto y Extremo, tal como esta descrito en el documento Metodología de Gestión de riesgos; cabe anotar que Global Suite facilita la identificación de dichos riesgos con los colores característicos, como es el caso del rojo para el nivel Extremo como se muestra en la Figura 4.

- Para las amenazas correspondientes a estos riesgos se asocian entonces los controles tomados de la Norma ISO 27001 que establecen un tratamiento de cada riesgo para lograr el NRA definido en el CNMH; estos controles están dentro de la Declaración de aplicabilidad del SGSI y se replican en los diferentes activos, como se puede evidenciar en la herramienta Global Suite.

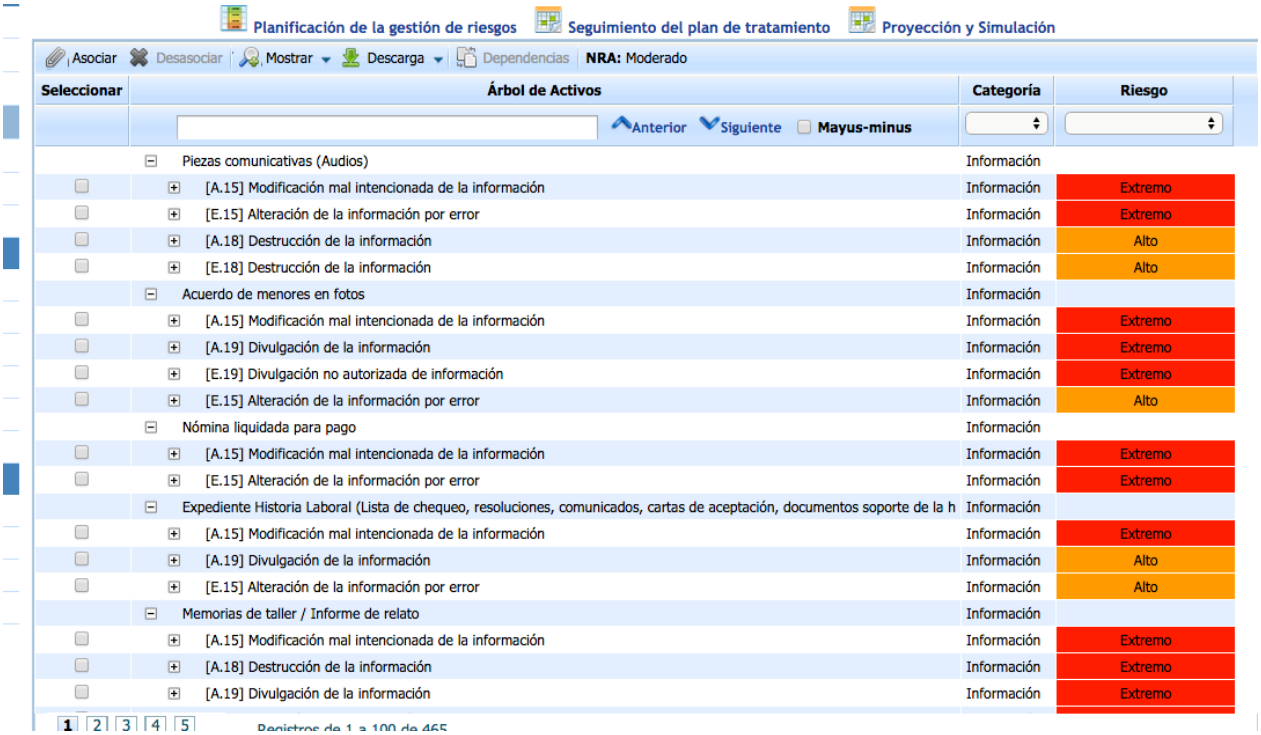

Figura 4. Riesgos que deben ser tratados

- El proceso de asociación de los controles con las amenazas se realiza con la opción “Controles Propuestos” dentro del panel inferior como se muestra en la Figura 5, en donde se debe seleccionar por cada control, **todas las amenazas** de todos los activos para los cuales dicho control aplique.

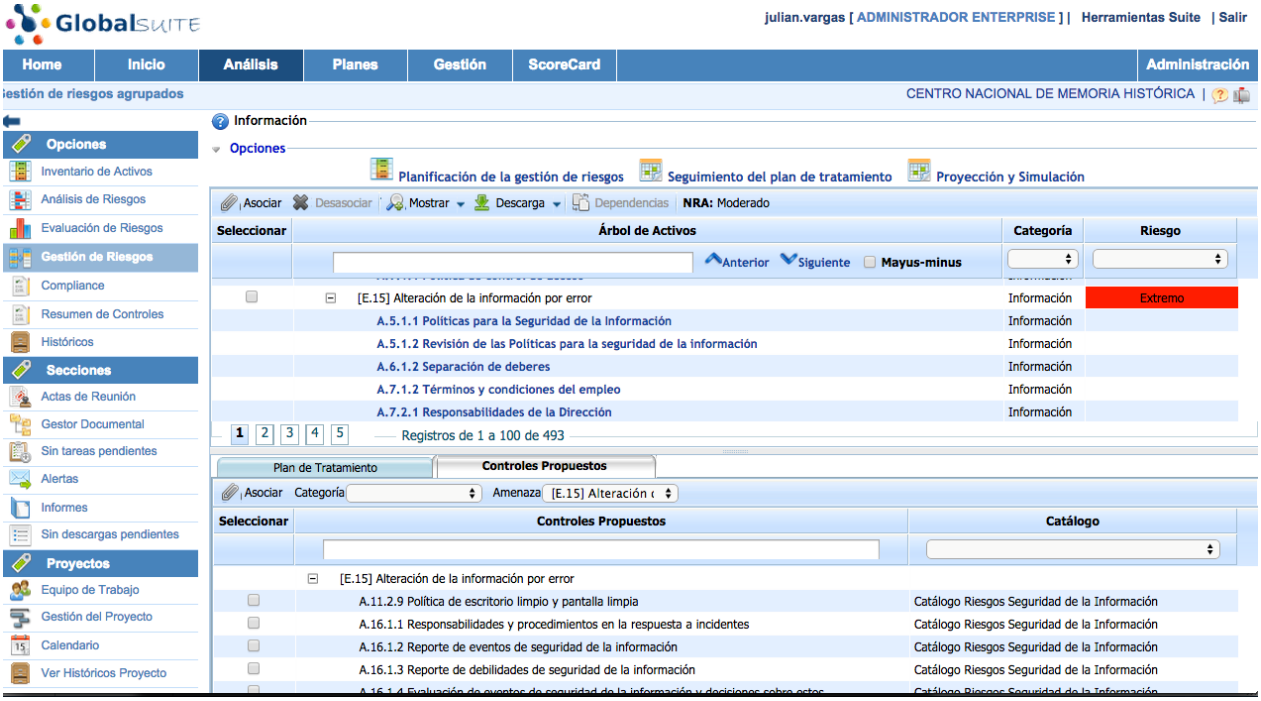

Figura 5. Controles Propuestos

- Una vez hecha la asociación de los controles con las amenazas para los que se va a a tratar los riesgos por encima del NRA, se procede con la especificación del Responsable del Control, los recursos y el plazo para su ejecución, tal como se muestra en la figura 6.

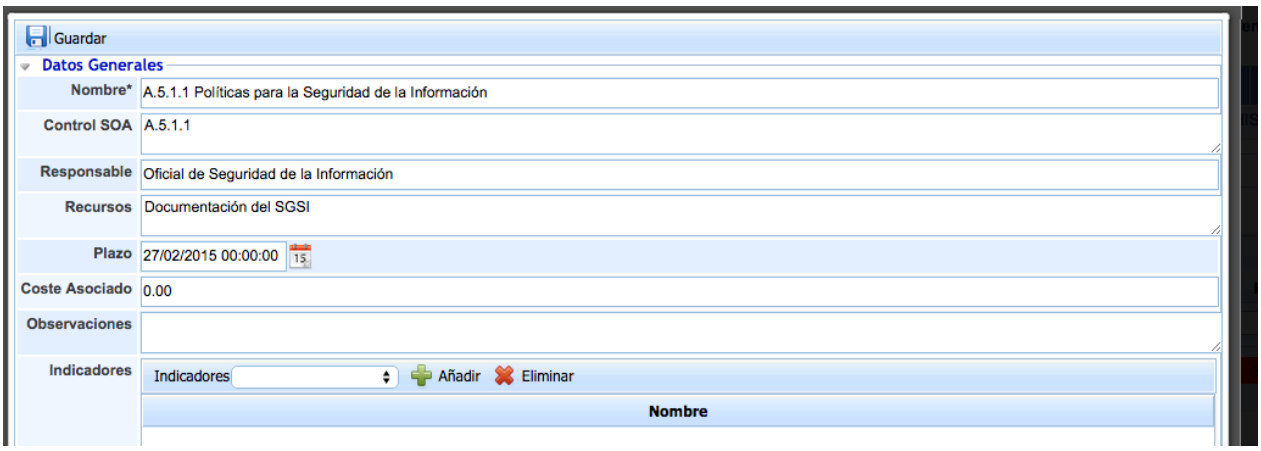

Figura 6. Definición del Control

- A continuación, se procede con la definición de las actividades requeridas para la implementación de cada Control establecido, en este se menciona la actividad, el responsable, los recursos y el plazo establecido para lograrlo tal como se muestra en la figura 7.

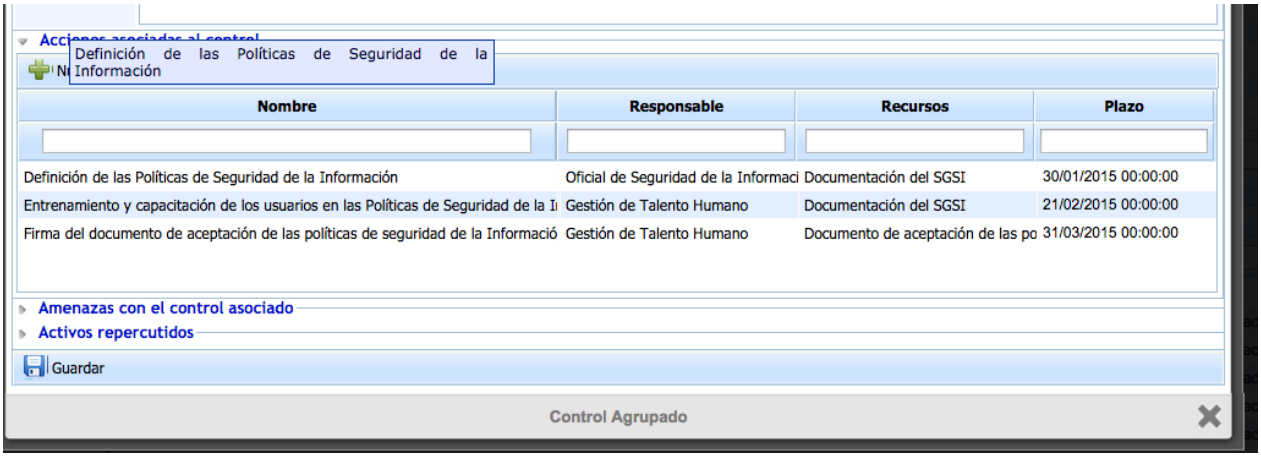

Figura 7. Actividades específicas del Control

2.3. REPORTE GENERADO

Para generar el listado completo de los controles que conforman el Plan de Tratamiento con los datos configurados en Global Suite se siguen los siguientes pasos:

- En el menú principal de Global Suite se escoge la opción Análisis
- En el menú de Análisis, se va a la parte de Opciones y se selecciona Gestión de Riesgos
- Dentro de la opción Gestión de Riesgos se selecciona la opción Análisis de CENTRO NACIONAL DE MEMORIA HISTÓRICA

Esto genera una ventana con dos secciones, en donde en la parte inferior se selecciona la opción Descarga y en esta "Informe.Docx" tal como se muestra en la Figura 8.

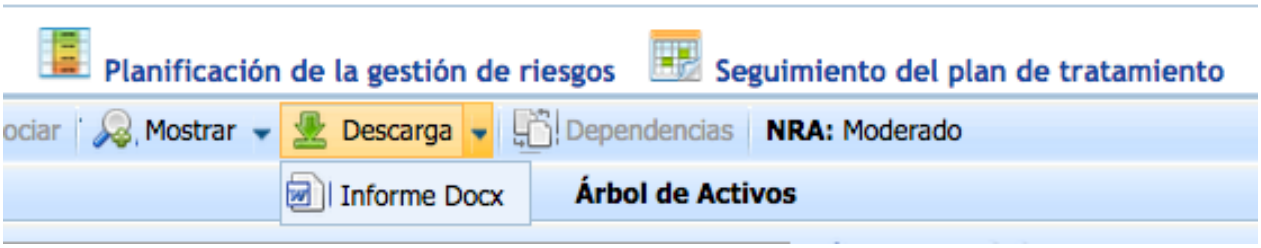

Figura 8. Generación del Reporte

- El informe generado se adjunta en este documento con el nombre generado automáticamente por Global Suite que tiene el siguiente formato Plan_Tratamiento_AñoMesDíaConsecutivo. Este reporte

presenta el listado de todos los controles que deben implementarse para mitigar los riesgos identificados y contiene los datos del Responsable del Control, Recursos, Plazo y las actividades necesarias igualmente con su responsable, recursos, responsable y plazo asignado.

3. CONCLUSIONES

- El primer paso para que sea la piedra angular del Plan de Tratamiento de Riesgos y como tal del SGSI es la formalización a través del acto administrativo, con el cual se van a soportar todas las labores recomendadas y se evidenciará el compromiso de la Dirección General.

- A partir de la formalización del SGSI, los funcionarios y proveedores del CNMH deben firmar los acuerdos y formatos correspondientes que corroboren que entienden y aceptan las nuevas responsabilidades que le son asignadas y que su incumplimiento puede llevar a un Proceso disciplinario o de tipo legal.

- El Plan de Tratamiento propuesto en Global Suite se soporta en las Políticas y Procedimientos que componen el SGSI y que fueron entregados como parte de los resultados de la Consultoría.

- Se deben priorizar las labores de sensibilización y entrenamiento de los Funcionarios considerando las vulnerabilidades evidenciadas por la carencia de una Cultura de seguridad de la información y que con la implementación del SGSI cada funcionario adquiere nuevas responsabilidades para las cuales debe adquirir nuevos conocimientos y habilidades.

- El CNMH debe asumir que a partir de la implementación del SGSI se establece un perfil mínimo que todos los Funcionarios y Proveedores de la Entidad, deben cumplir para poder alinearse con las exigencias para la protección de la confidencialidad, integridad y disponibilidad de la información con base en la clasificación establecida.

- Es importante considerar que en la medida que se permita que los Funcionarios hagan uso del soporte técnico dispuesto por la Entidad, por carencias en su Cultura de Seguridad o conocimientos técnicos mínimos, esto seguirá generando vulnerabilidades que expondrán la seguridad de la información.

- Se debe replantear la relación con todos los proveedores para que se cumpla con la Política de Seguridad de la Información establecida.

- Cuando se evidencie que no es posible cumplir con un control definido por el SGSI por razones de presupuesto o asignación de recursos, se debe escalar dicha situación hasta el nivel de autoridad suficiente para que se asuman los riesgos que esto conlleve.

- Considerando el arduo trabajo que representa la implementación del SGSI, se debe trabajar priorizando los esfuerzos con base en la calificación de los riesgos, es decir empezando por los catalogados como Nivel Extremo.

- La inversión que se requiere en cuanto a Tecnología de Información y comunicaciones para implementar controles de seguridad está justificada por la mitigación de riesgos exigida por la Entidad. Mientras no se adquieran las soluciones correspondientes el CNMH convivirá con riesgos que no son aceptables y esto debe ser escalado al nivel de autoridad que apruebe dicha situación o que en caso contrario aplique las medidas correspondientes.

CONTROL DE CAMBIOS			
ACTIVIDADES QUE SUFRIERON CAMBIOS	**CAMBIOS EFECTUADOS**	**FECHA DE CAMBIO**	**VERSIÓN**
No Aplica	Elaboración de Documento	30-11-2017	001