PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL HOSPITAL MILITAR CENTRAL

MAYOR GENERAL MÉDICO
CLARA ESPERANZA GALVIS DÍAZ
DIRECTORA GENERAL
HOSPITAL MILITAR CENTRAL

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PRESENTACIÓN

El presente documento contiene el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Hospital Militar Central. La información que resguarda crea, procesa y gestiona el Hospital Militar Central es crucial para el normar desarrollo y prestación adecuada de los servicios. Es por esto por lo que es obligación para el Hospital Militar Central resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos.

Por lo anterior y dentro de Marco de Seguridad del Modelo de Seguridad y Privacidad de la información, un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. Es importante resaltar que este plan esta alineado con la guía de riesgos del DAFP[1] con el fin de que exista integración a otros modelos de gestión que existan en el Hospital Militar Central.

[1] Departamento de la Función Pública - DAFP

TABLA DE CONTENIDO

OBJETIVO

Definir el plan de tratamiento de riesgos que hacen parte del Sistema de Gestión de Seguridad de la Información, para así aplicar los controles con los cuales se buscan mitigar su materialización en el Hospital Militar Central.

ALCANCE

Se define el alcance del presente plan de tratamiento de riesgos, será aplicable a todos los procesos estratégicos, misionales, de apoyo y de evaluación propios o de terceros que creen, procesen, transmitan o resguarden información clínica de nuestros usuarios, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información

TERMINOS Y DEFINICIONES

- **Información:** Información almacenada o procesada física o digitalmente " Bases de datos, archivos de datos, contratos, acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación o capacitación, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoria e información archivada)

- **Software:** Aplicaciones, herramientas de desarrollo, utilidades

- **Hardware:** son activos físicos como, por ejemplo, equipos de cómputo y de comunicaciones, medios removibles, entre otros que por su criticidad son considerados activos de la información, no solo activos fijos)

- **Servicios:** Servicios de computación y comunicaciones, tales como Internet, correo electrónico, páginas de consulta, directorios compartidos e intranet, entre otros

- **Personas:** Aquellas personas que, por su conocimiento, habilidades, experiencia y criticidad para el proceso, son consideradas activos de la información.

- **Imagen y reputación:** Good Will o reconocimiento público que debe ser protegido.

- **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.

- **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.

- **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

PLAN DE TRATAMIENTO DE RIESGOS

Con el ánimo de asegurar el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información - SGSI, prevenir y reducir los efectos indeseados a la hora de materializarse un riesgo que afecte un activo de la información, procurar la mejora continua, definir acciones para tratar los riesgos de seguridad de la información y evaluar la eficacia de las acciones tomadas; el Hospital Militar Central identificará y clasificará los activos de la información, identificará los riesgos de seguridad de la información y definirá las acciones a tomar bajo las siguientes premisas:

PROCESO DE IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN

El Hospital Militar Central identificará toda información o todo activo que la contenga así:

- **Información:** Información almacenada o procesada física o digitalmente " Bases de datos, archivos de datos, contratos, acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación o capacitación, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoria e información archivada)
- **Software:** Aplicaciones, herramientas de desarrollo, utilidades
- **Hardware:** son activos físicos como, por ejemplo, equipos de cómputo y de comunicaciones, medios removibles, entre otros que por su criticidad son considerados activos de la información, no solo activos fijos)
- **Servicios:** Servicios de computación y comunicaciones, tales como Internet, correo electrónico, páginas de consulta, directorios compartidos e intranet, entre otros
- **Personas:** Aquellas personas que, por su conocimiento, habilidades, experiencia y criticidad para el proceso, son consideradas activos de la información.
- **Imagen y reputación**: Good Will o reconocimiento público que debe ser protegido.

Para esta labor todos los responsables de los procesos deberán diligenciar la encuesta publicada en https://goo.gl/forms/fuqII5FRwYSMIcD83 de esta manera definiremos la matriz de activos de la información en los siguientes términos:

1. Identificación o etiquetado
2. Proceso al que corresponde
3. Descripción del activo
4. Tipo de activo
5. Contenedor
6. Responsable

Una vez identificado y realizado el inventario de activos de la información deberá ser clasificado con base a los criterios de clasificación definidos en el Manual de Contrainteligencia (MACI) FF.MM2-6-Reservado y resolución número 03049 de 2012 DIPON Manual de Sistema de Gestión de Seguridad de la Información, que define los siguientes niveles:

- Según su confidencialidad

Valor	Descripción
5	**Ultra secreto**: Información pertinente a actividades o planes de la Defensa Nacional interna o externa y a operaciones de inteligencia relativas a la misma, cuya divulgación autorizada podría conducir a un rompimiento diplomático que afecte los intereses de la nación, a un ataque armado contra la misma o a destruir su estabilidad interna.
4	**Secreto:** Información pertinente a actividades o planes de defensa nacional interna y operaciones de inteligencia relativa a la misma, cuya divulgación no autorizada podría afectar las relaciones internas, lesionar el prestigio del país o poner en peligro la estabilidad interna del mismo.
3	**Reservado**: Información cuya divulgación no autorizada puede ser perjudicial para los intereses o prestigio de la institución militar, proporcionar ventajas a la amenaza actual o potencial o causar bajas o pérdidas propias en acciones de Defensa Nacional.
2	**Confidencial:** Información que por su contenido solo interesa a quienes va dirigido y cuya divulgación no autorizada puede ocasionar perjuicios a determinada entidad o persona.
1	**Restringido/interno:** es aquella información dirigida a los miembros de la institución y que se debe proteger del conocimiento de personas extrañas a la misma.

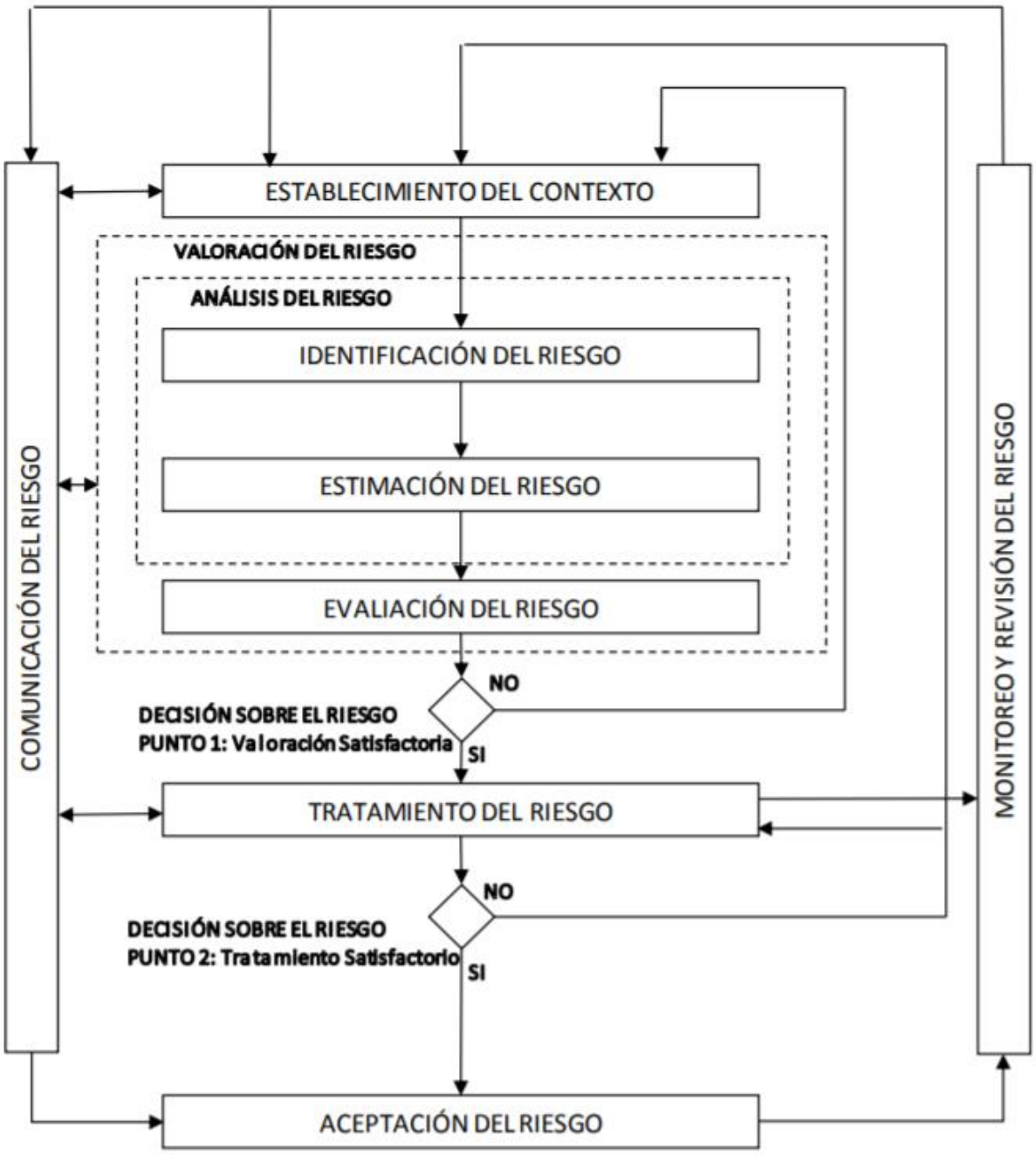
- Según su integridad

Valor	Descripción
5	No puede repararse y ocasiona pérdidas graves para el país.
4	No puede repararse y ocasiona pérdidas graves para la institución.
3	Difícil reparación y pérdidas significativas.
2	Puede repararse, pérdidas leves.
1	No afecta la operación y puede repararse fácilmente.

- Según su disponibilidad

Valor	Descripción
5	CRÍTICOS, la interrupción es de minutos y hasta 12 horas.
4	URGENTE, la interrupción hasta por 24 horas.
3	IMPORTANTE, interrupción hasta por 72 horas.
2	NORMAL, interrupción de hasta siete días.
1	NO ESENCIALES, la interrupción es de hasta 30 días

PROCESO DE VALORACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN



Tomado de: Norma ISO/IEC 27001:2013

El análisis de riesgos se realizará todos y cada uno de los procesos procesos estratégicos, misionales, de apoyo y de evaluación del Hospital Militar Central. Los riesgos asociados a la seguridad de la información que se identifiquen a los activos de la información identificados deberán ser tratados de la siguiente manera:

1. Se realizarán entrevistas con los responsables de los activos con el fin de dar a conocer la metodología y hacer la valoración de los diferentes riesgos en términos de probabilidad e impacto.
2. Realizar el Análisis y evaluación de los riesgos de seguridad de la información para todos los activos de la información.
3. Se realizará la Identificación de opciones de tratamiento de riesgos.
4. Se realizará de manera formal una reunión para la comunicación de resultados al Comité de Seguridad de la Información.
5. El análisis y evaluación de riesgos deberá hacerse al menos una vez al año y cada vez que ocurran cambios significativos en la estructura orgánica de las dependencias y entidades que conforman el Hospital Militar Central, en la plataforma tecnológica, en los procesos, entre otros.
6. Para la valoración de los riesgos se tendrá en cuenta lo relacionado al cabal cumplimiento de:

ACCIONES PARA MITIGAR LOS RIESGOS

Resultado (de acuerdo a la Valoración)	Acción a Tomar	Observaciones
ALTO	Mitigar, Transferir o Compartir	
MEDIO	Mitigar, Transferir o Compartir	
BAJO	ACEPTAR	Se debe cuantificar la materialización del riesgo

CRITERIOS PARA LA VALORACION DE RIESGOS

Probabilidad (Frecuencia)

Criterio	Valoración	Observaciones
3	ALTO	Puede Suceder en cualquier momento
2	MEDIO	Ha sucedido al menos una vez en el último año
1	BAJO	No ha sucedido en el último año

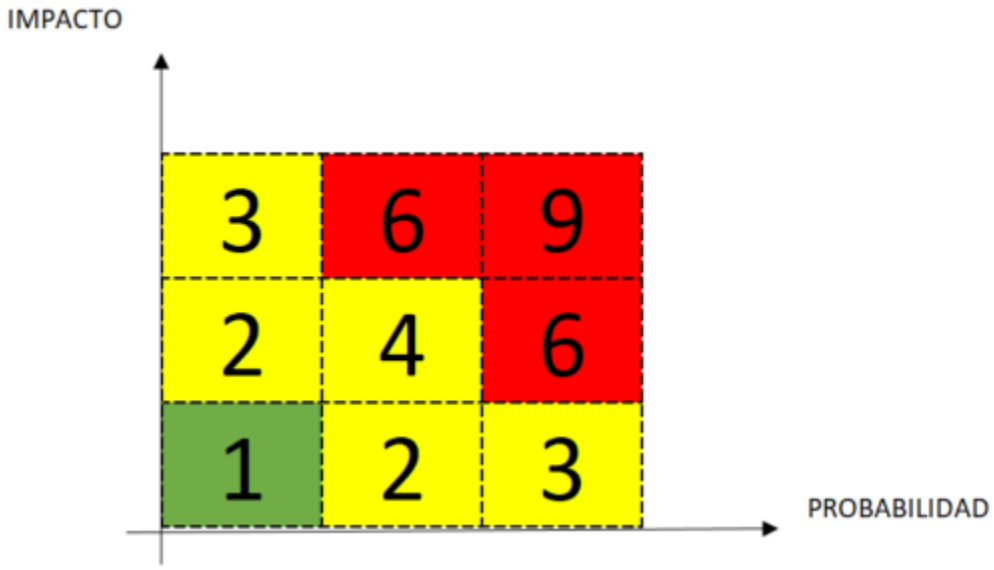
Impacto

Criterio	Valoración	Observaciones
3	ALTO	**Financiero:** Costo no Presupuestado **Legal:** Demanda o proceso legal **Reputación:** Afectación de Imagen pública, medios de comunicación **Operativo:** Afectación en al menos 1 proceso misional del HMC.
2	MEDIO	**Financiero:** Costo que afecta el presupuesto, pero puede ser cubierto. **Legal:** Queja o Reclamo del usuario, cliente o dueño de la información. **Reputación:** Imagen del HMC afectada internamente o para un usuario especifico.

		Operativo: Solo se afectan procesos o servicios de Apoyo.
1	BAJO	**Financiero:** No Costo **Legal:** No Demanda **Reputación:** No afectación a la Imagen del HMC **Operativo:** No afecta la Operación

$$riesgo = Probabilidad * Impacto$$

VALORACION DEL RIESGO



ESCALA DE PRIORIZACION DEL RIESGO

Resultados	valoración	Prioridad
1	BAJO	C
2,3,4	MEDIO	B
6 y 9	ALTO	A

ACCIONES PARA MITIGAR LOS RIESGOS

Resultado (de acuerdo con la Valoración)	Acción a Tomar	Observaciones
ALTO	Mitigar, Transferir o Compartir	Se deben determinar acciones inmediatas que permitan tratar de manera adecuada el riesgo.
MEDIO	Mitigar, Transferir o Compartir	En este caso se determinarán los controles establecidos en la norma ISO /IEC 27001 Anexo A, transferir con una Póliza o Cláusulas contractuales.
BAJO	ACEPTAR	Se debe cuantificar la materialización del riesgo y asumir

La materialización de los riesgos puede ser a causa de diferentes amenazas; en el sistema de gestión de seguridad de la información del Hospital Militar Central, los riesgos de seguridad de la información serán valorados mínimo desde el punto de vista de las siguientes amenazas:

1. **De origen natural:** Fuego, inundación, desastre natural (sismo, Siniestro, meteorológico)
2. **De Origen Industrial:** Fuego, daños por agua, desastres industriales (explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tránsito), contaminación mecánica (polvo, vibraciones, suciedad), contaminación electromagnética (interferencias de radio, campos magnéticos, luz ultravioleta).
3. **Del entorno:** avería física o lógica (fallos en los equipos, fallos en los programas), corte del suministro eléctrico, condiciones inadecuadas de temperatura o humedad, Fallo en servicios de comunicaciones, interrupción de otros servicios esenciales (Papel, impresora), errores o fallos intencionados por humanos, errores del administrador, errores de configuración, deficiencias de la organización, difusión de software dañino (virus, troyanos, etc,), fugas de información, alteración accidental de la información, destrucción de la información, caída del sistema, perdida de equipos, indisponibilidad del personal.
4. **Ataques Intencionados:** Manipulación de registros, manipulación de la configuración, Suplantación de identidad, Abuso de privilegios de acceso, Uso no previsto, difusión de software dañino, errores de comunicación, acceso no autorizado, repudio, interceptación de información, modificación de la información, destrucción de la información, divulgación de la información, manipulación de programas y/o equipos, denegación de servicio, robo, ataque destructivo, ocupación enemiga, indisponibilidad del personal, ingeniería social, extorsión.

El resultado de esta fase se verá reflejado en una tabla como la siguiente:

Riesgo	Activo	Nombre del activo	Amenaza	Vulnerabilidad	Nivel de Riesgo	Valoración	Probabilidad de ocurrencia	Impacto	Opcion de Tratamiento	Controles	Eficacia	Riesgo Residual	Firma de Aceptacion Riesgo
R1													
R2													
R3													
R4													

Tabla N° 1 – Plan de Tratamiento del Riesgo

Contoles	Descripcion del Control	Aplica	Justificacion	¿Esta Implementado?	Resónsable de la aplicación	Escala de Madurez

Tabla N° 2 – Declaración de Aplicabilidad

MEDICIÓN DE LA EFICACIA

Con el fin de medir la madurez de cada control y conocer de manera adecuada la eficacia de la aplicación de uno o más controles a determinado riesgo se define la siguiente escala de valoración.

Valoración	Descripción
1	No tengo nada
2	El control está considerado y documentado

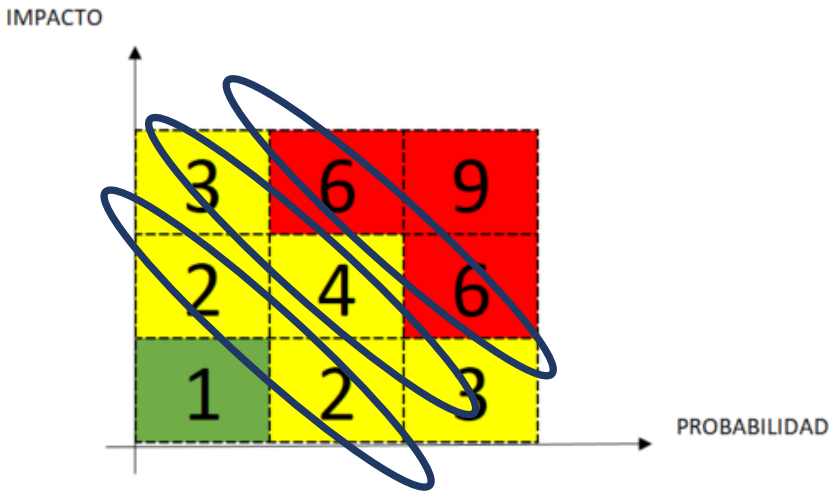
3	El control esta implementado, documentado y es funcional.

A cada control se le debe dar una valoración y entendiendo que a la mitigación de un riesgo se le pueden asociar uno o varios controles mediremos la eficacia así:

$$Eficacia = \sum_{i=n}^{n} xi/n$$

Por lo anterior y teniendo en cuenta los resultados calcularemos el Riesgo Residual así:

1. Si Eficacia = 1, entonces el Riesgo Residual = Riesgo Inherente
2. Si Eficacia = 2, entonces el Riesgo Residual = Riesgo Inherente – 1 nivel valoración de riesgo
3. Si Eficacia = 3, entonces el Riesgo Residual = Riesgo Inherente – 2 niveles de valoración de riesgos



Aceptación de los riesgos residuales

Los responsables de los activos de la información aceptaran de manera formal los riesgos residuales y serán los responsables de realizar el inventario de activos de la información mínimo una vez al año y que se realice la adecuada valoración de riesgos de seguridad de la información.

MARCO LEGAL

- Ley 527 de 1999 “Comercio Electrónico”
- Ley 594 de 2000 “Ley General de Archivo”
- Ley 603 de 2000 “Control de legalidad del software”.
- Ley 734 de 2002 “Código Disciplinario Único”.
- Ley 836 de 2003 “Régimen Disciplinario FF.MM”.
- Ley 1266 de 2008 “Por lo cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información”.
- Ley 1273 de 2009 “Protección de la Información y de los Datos”.

- Documento CONPES 3701 de julio del 2011 “Lineamientos de política para ciberseguridad y ciberdefensa”.
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” y su decreto reglamentario 1377 del 27 de junio de 2013.
- Reglamento Interno de Trabajo
- 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
- Y las demás normas vigentes aplicables.

REQUISITOS TECNICOS

- Modelo de Privacidad y Seguridad de la información del MINTIC.
- Norma Técnica Colombiana NTC – ISO/IEC 27000:2016

DOCUMENTOS ASOCIADOS

- Política de seguridad y Privacidad de la Información
- Directiva de control de acceso
- Plan de Sensibilización de Seguridad de la Información
- Directiva de Backup
- Directiva de Uso apropiado de correo electrónico
- Política de tratamiento de datos personales
- Directiva de reuniones

RESPONSABLE DEL DOCUMENTO

- Jefe Unidad de Informática
- Coordinador Área Gestión de Seguridad de la Información

Teniente **Coronel Ariadna Ramirez Ospina**
Jefe de Unidad de Seguridad y Defensa
Unidad de Informatica