POLITICA DE SEGURIDAD INFORMATICA – HOSPITAL MILITAR CENTRAL

1. DEFINICION

Con el fin de proteger los activos informáticos de la institución, se hace necesario la generación y puesta en marcha de una política de seguridad que nos permita mejorar la forma de usar los activos informáticos que la entidad posee, la política de seguridad del Hospital Militar Central da lugar a que en los últimos años se han venido adquiriendo nuevas tecnologías que nos permiten la comunicación con el mundo exterior, a su vez esto trae nuevas amenazas para las cuáles debemos estar preparados y capacitados para afrontarlas.

Hoy en día la red de comunicaciones del Hospital Militar Central, tiene la capacidad de comunicarse e interconectarse a otras redes, podemos mejorar nuestra productividad y mejorar sustancialmente la atención de los usuarios, acortando distancias y mejorando la respuesta a trámites, por ende, estas nuevas formas de comunicación traen consigo además de muchas bondades, amenazas. La política de seguridad del Hospital Militar Central abarca la seguridad lógica y la seguridad física de todos los procesos del Hospital Militar Central, ofreciendo siempre la Integridad, la Disponibilidad, y la Confidencialidad.

La política de seguridad del Hospital Militar Central, establecerá un cómo proceder en cuanto al uso de los activos informáticos que la entidad pone a disposición de sus colaboradores para la atención de los usuarios.

La información que por la red del Hospital Militar viaja es el activo más importante con que la entidad cuenta, por ende todo el personal que hace uso de ella debe conocer y cumplir las reglas del buen y correcto uso del mismo.

2. ALCANCE

Con esta Política se pretenden generar lineamientos de buen y correcto uso de los activos informáticos puestos a disposición del personal que labora en el Hospital Militar Central, con el fin de mejorar el desarrollo de los diferentes procesos que intervienen para la correcta y eficaz atención al usuario. Lo anterior alineado con la normatividad actual y vigente así como con la directiva permanente impartida por el Ministerio de Defensa Nacional de seguridad informatica.

El presente documento define la estructura de la organización de seguridad de la información, funciones, controles de uso aceptables y las directrices para el sistema de gestión de seguridad de la información para el Hospital Militar Central.

Las políticas establecidas y sus posteriores actualizaciones aplican a todos los recursos y activos de información del Hospital Militar Central y son de obligatorio cumplimiento.

3. OBJETIVOS

- Mitigar la perdida de información que se encuentra en la Red del Hospital Militar Central.
- Educar a los usuarios finales de la red HOMIC, sobre el correcto y buen uso de los activos informáticos que brinda la institución para el normal curso de las actividades cotidianas.
- Establecer los lineamientos a seguir por los actores que intervienen a diario en el uso de los activos informáticos del Hospital Militar Central.
- Establecer las sanciones a que hay lugar por el no cumplimiento de esta política.
- Definir las vulnerabilidades y riesgos de la red HOMIC.
- Definir los procedimientos, políticas y normas que se deben acatar para el buen y correcto uso de los activos informáticos del Hospital Militar Central, así como el uso de la red HOMIC.
- Definir los responsables de todos y cada uno de los procesos en donde intervienen activos informáticos de la institución.
- Definir los riesgos de la red HOMIC y de los activos informáticos de la institución.
- Establecer y difundir los criterios y comportamientos que deben seguir todos los funcionarios directos, temporales, contratistas, practicantes, terceros o cualquier persona que tenga una relación contractual con el Hospital Militar Central, o que tenga acceso a los activos de información con el propósito de preservar la Confidencialidad, Integridad y Disponibilidad de la información a fin de fortalecer la continuidad de las actividades administrativas, operativas y logísticas de la entidad.
- Proteger adecuadamente la información, reduciendo los riesgos y optimizando la inversión en tecnologías de información.
- Proteger los recursos de información y tecnología utilizados para su procesamiento, frente a amenazas internas y externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad, mediante la implementación de controles efectivos.
- Establecer un modelo organizacional de seguridad de la información, definiendo claramente los roles y responsabilidades de los que intervienen en la implementación de la política.
- Promover, mantener y realizar mejoramiento continuo del nivel de cultura en seguridad de la información, así como lograr la concientización de todos los funcionarios y contratistas y demás personas que interactúen con el Hospital

Militar Central, para minimizar la ocurrencia de incidentes de seguridad de la información.

- Mantener la política de seguridad actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

4. REFERENCIAS NORMATIVAS

a. Constitución Política de Colombia
b. Ley 80 de 1993 "Estatuto general de contratación de la administración pública".
c. Ley 87 de 1993 "Control Interno en los organismos del Estado".
d. Ley 527 de 1999 "Comercio Electrónico"
e. Ley 594 de 2000 "Ley General de Archivo"
f. Ley 599 de 2000 "Código Penal Colombiano".
g. Ley 603 de 2000 "Control de legalidad del software".
h. Ley 734 de 2002 "Código Disciplinario Único".
i. Ley 836 de 2003 "Régimen Disciplinario FF.MM".
j. Ley 1015 de 2006 "Régimen Disciplinario para la Policía Nacional".
k. Ley 1266 de 2008 "Por lo cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información".
l. Ley 1273 de 2009 "Protección de la Información y de los Datos".
m. Documento CONPES 3701 de julio del 2011 "Lineamientos de política para ciberseguridad y ciberdefensa".
n. 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.
o. Manual de Contrainteligencia FF.MM. 2-6 Reservado.
p. Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional de la Republica de Colombia.
q. Resolución No. 03049 del 24 de agosto de 2012, por la cual se adopta el Manual del Sistema de Gestión de Seguridad de la Información.
r. Norma Técnica Colombiana NTC – ISO/IEC 27000
s. Metodología para Análisis y Evaluación de Riesgos UGG.

Y las demás normas vigentes aplicables.

5. VIGENCIA

Las disposiciones contenidas en el presente documento, empezarán a regir a partir de la fecha de su expedición y deroga lo contenido en la resolución 036 del 06 de Febrero de 2006 y las demás normas que le sean contrarias.

6. MARCO DE REFERENCIA

Teniendo en cuenta el estándar adoptado por el sector defensa la política de seguridad del Hospital Militar Central adopta también la familia de normas de la serie ISO 27000 como marco de referencia para la implementación de su sistema de gestión de seguridad de la información.

ISO 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización. Entre las distintas normas que componen la serie ISO 27000 y que fueron tomadas como referente, se resaltan: ISO/IEC 27001:2005 sobre los requisitos para el establecimiento del sistema de gestión de seguridad de la información, ISO/IEC 27002:2005 - Código de práctica para la gestión de la seguridad de la información e ISO/IEC 27005:2008 relacionada con la gestión del riesgo.

7. MISIONES PARTICULARES

7.1 DIRECTOR GENERAL

a. Verificar el cumplimiento del presente documento, en particular la difusión y adopción de las políticas, normas y estándares de seguridad de la información.

b. Promover el desarrollo de una cultura de seguridad de la información a través de campañas de sensibilización y concientización.

c. Implementar, apoyar y soportar el Sistema de Gestión de Seguridad de la Información.

d. Apoyar los programas de capacitación, actualización y entrenamiento técnico del personal de la Unidad de Informática en temas relacionados con seguridad de la información.

e. Nombrar al oficial de seguridad de la información (OSI) como integrante del Comité de Seguridad de la Información y apoyar las iniciativas de seguridad que se definan sobre los activos de información.

f. Gestionar los recursos financieros requeridos para la apropiada protección de los activos de información y mantenimiento del sistema de gestión de seguridad de la información.

g. Ordenar la inclusión de temas relacionados con seguridad de la información en las materias de tecnología que se dictan en las escuelas de formación y capacitación.

h. Apoyar la aplicación y cumplimiento de las recomendaciones emitidas por el comité de seguridad de la información.

7.2UNIDAD DE INFORMATICA

a. Promover el cumplimiento por parte del personal que conforma la Unidad de las políticas de seguridad de la información.

b. Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de seguridad de la información.

c. Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de seguridad de la información.

d. Diseñar, desarrollar, instalar y mantener las aplicaciones bajo su responsabilidad de acuerdo con la metodología establecida e incluyendo los controles de seguridad de la información desde el diseño.

e. Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo.

f. Implementar y administrar los controles de seguridad sobre la información y conexiones de las redes de datos bajo su administración.

g. Definir e implementar la estrategia de concientización y capacitación en seguridad de la información para los funcionarios, contratistas y demás terceros, cuando aplique.

h. Custodiar la información y los medios de almacenamiento bajo su responsabilidad.

i. Garantizar la implementación de las recomendaciones generadas en los análisis de vulnerabilidades.

j. Gestionar la plataforma tecnológica que soporta los procesos de la entidad.

k. Definir, mantener y controlar la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones

de trabajo de los usuarios; así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

l. Gestionar la adquisición de software y hardware.

m. Entregar los equipos de cómputo a los funcionarios y/o contratistas.

n. A través de las áreas de Seguridad de la Información se debe:

1) Monitorear y evaluar los procesos o actividades sobre las plataformas tecnológicas, delegados en terceros.

2) Establecer, verificar, monitorear y validar los procedimientos de continuidad y de contingencia para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.

3) Establecer, documentar y dar mantenimiento a los procedimientos de seguridad de la información que apliquen para la plataforma de tecnologías de información administrada por esta oficina.

4) Solucionar los incidentes de seguridad de la información que se presenten en la entidad.

5) Realizar análisis de vulnerabilidades a la plataforma tecnológica con el fin de generar recomendaciones.

o. Conformar y liderar el equipo de respuesta a emergencias informáticas y centros de operaciones de seguridad con el fin de apoyar la gestión de incidentes de seguridad informática que se llegasen a presentar en el Hospital Militar Central.

7.3UNIDAD DE TALENTO HUMANO - *Ref: ISO/IEC 27001:2005 CL. A.8.1.2. e ISO/IEC 27002:2002 CL. 8.1.3*

a. Comunicar los derechos y establecer las responsabilidades legales que adquiere cada funcionario, contratista y/o tercero, con relación al manejo y protección de los datos institucionales tanto al interior como fuera de las

b. Realizar auditorías a los procesos del Sistema de Gestión de Seguridad de la Información por lo menos una vez al año, de acuerdo a lo establecido en la norma ISO 27001.

7.5OFICINA DE SEGURIDAD

a) Elaborar y actualizar los estudios de seguridad de personal (ESP), las promesas de reserva, las pruebas técnicas de confidencialidad y/o las tarjetas de autorización para manejo de documentación clasificada, de los funcionarios que laboran en áreas donde se maneja información sensible y/o clasificada.

b) Elaborar y actualizar los estudios de seguridad de personal (ESP) y las promesas de reserva, del personal contratista y/o asesor externo que requiera interactuar con los activos de información del Hospital Militar Central.

c) Verificar las actividades de monitoreo del uso de los activos de información para prevenir el impacto de los riesgos derivados de pérdida de integridad, disponibilidad y confidencialidad de la información.

d) Supervisar el cumplimiento de los procedimientos y controles para evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información del Hospital Militar Central.

7.6JEFES DE AREA Y/O UNIDAD

a. Documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados con sus procesos, incluyendo aquellas actividades que sean consideradas como controles de seguridad de la información dentro de dichos procedimientos.

7.7DUEÑOS O RESPONSABLES DE LOS ACTIVOS DE INFORMACION

a. Clasificar los activos de información bajo su responsabilidad de acuerdo con los requerimientos de confidencialidad, integridad y disponibilidad, verificar que se les proporcione un nivel adecuado de protección en conformidad con los estándares, políticas y procedimientos de seguridad de la información.

b. Definir los acuerdos de niveles de servicio para recuperar sus activos de información y sistemas críticos e identificar los impactos en caso de una interrupción extendida.

instalaciones del Hospital Militar Central (políticas de seguridad de la información).

b. Incluir en los contratos cláusulas de confidencialidad y no divulgación de la información, así como la obligatoriedad en el cumplimiento de la política de seguridad de la información del Hospital Militar Central.

c. Garantizar que se realicen las verificaciones y controles de seguridad requeridos por la criticidad del empleo, tales como verificación de antecedentes judiciales, validación de certificados de estudios presentados, validación de referencias de comportamiento satisfactorio y validación de su hoja de vida.

d. Definir claramente las funciones y tareas que desempeñará el funcionario en el cargo con el fin de establecer la responsabilidad en el manejo de la información teniendo en cuenta la clasificación de la misma y el cumplimiento de las políticas de seguridad de la información.

e. Elaborar y ejecutar programas de inducción y de re-inducción para los funcionarios asegurando que conozcan sus responsabilidades e implicaciones por el uso indebido de activos de información o de otros recursos informáticos, haciendo énfasis en las consecuencias jurídicas que puede acarrear al servidor público.

f. Gestionar los aspectos de seguridad que se requieran durante el proceso de desvinculación de cualquier empleado, y demás novedades de personal, informando a la Unidad de Informática con el fin de que se tomen las medidas y procedimientos de entrega de hardware, software e información a su cargo, necesarios para evitar riesgos que atenten contra la seguridad de la información.

g. Dar cumplimiento a los artículos establecidos en la Ley Estatutaria N°. 1581 de 17 de octubre del 2012 por la cual se dictan disposiciones generales para la protección de datos personales.

7.4OFICINA DE CONTROL INTERNO

a. Validar la aplicación y cumplimiento de las políticas de Seguridad de la Información definidas en este documento, la aplicación de controles sobre los activos de información y los requerimientos del Sistema de Gestión de Seguridad de la Información.

c. Definir los requerimientos de continuidad y de recuperación en caso de desastre.

d. Coordinar un análisis de riesgos por lo menos una vez al año, para determinar el grado de exposición a las amenazas vigentes y confirmar los requerimientos de confidencialidad, integridad y disponibilidad relacionados con sus activos de Información.

e. Comunicar sus requerimientos de seguridad de información al líder del Área de Seguridad de la Información del Hospital Militar Central.

f. Determinar y autorizar todos los privilegios de acceso a sus activos de información.

g. Comunicar al Área de Seguridad de la Información sus requerimientos en capacitación sobre seguridad de información.

h. Revisar los registros y reportes de auditoría para asegurar el cumplimiento con las restricciones de seguridad para sus activos de información. Estas revisiones podrán realizarse en coordinación con el custodio del activo; sin embargo, se deben verificar los resultados de las revisiones y reportar cualquier situación que involucre un incumplimiento o violación a la seguridad de Información, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.

i. Participar en la resolución de los incidentes relacionados con el acceso no autorizado o mala utilización de los activos de información bajo su responsabilidad, incluyendo los incumplimientos a la disponibilidad, confidencialidad e integridad.

7.8 FUNCIONARIOS, CONTRATISTAS Y TERCEROS

a. Cumplir con las políticas de seguridad de la información, contempladas en el presente documento.

b. Velar por el cumplimiento de las políticas de seguridad de la información dentro de su entorno laboral inmediato.

c. Reportar de manera inmediata y a través de los canales establecidos, la sospecha u ocurrencia de eventos considerados incidentes de seguridad de la información, de acuerdo al procedimiento de Gestión de Incidentes de Seguridad de la Información.

d. Utilizar los sistemas de información y el acceso a la red únicamente para los propósitos que lo vinculan.

e. Utilizar únicamente software y demás recursos tecnológicos autorizados.

8. ACCIONES QUE AFECTAN LA SEGURIDAD DE LA INFORMACIÓN

A continuación se describen algunas acciones identificadas que afectan la seguridad de la información, y que ponen en riesgo la disponibilidad, confidencialidad e integridad de la misma, así:

a. Dejar los computadores encendidos en horas no laborables.

b. Permitir que personas ajenas a las dependencias y entidades del Sector Defensa, ingresen sin previa autorización a las áreas restringidas o donde se procese información sensible.

c. No clasificar y/o etiquetar la información.

d. No guardar bajo llave, documentos impresos que contengan información clasificada, al terminar la jornada laboral.

e. Hacer uso de la red de datos del Hospital Militar Central para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.

f. Instalar software en la plataforma tecnológica del Hospital Militar Central, cuyo uso no esté autorizado por la Unidad de Informática, que puedan atentar contra las leyes de derechos de autor o propiedad intelectual.

g. Destruir la documentación institucional, sin seguir los parámetros y normatividad vigente establecida para el proceso de gestión documental.

h. Descuidar información clasificada del Hospital Militar Central, sin las medidas apropiadas de seguridad que garanticen su protección.

i. Enviar información clasificada como no pública del Hospital Militar Central, a través de correos electrónicos personales, diferentes a los institucionales.

j. Enviar información clasificada como no pública por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.

k. Guardar información clasificada en cualquier dispositivo de almacenamiento que no pertenezca al Hospital Militar Central.

l. Conectar computadores portátiles u otros dispositivos electrónicos personales a la red de datos del Hospital Militar Central, sin la debida autorización.

m. Ingresar a la red de datos del Hospital Militar Central, por cualquier servicio de acceso remoto sin la autorización de la Unidad de Informática.

n. Usar servicios de internet en los equipos de la institución, diferente al provisto por la Unidad de Informática.

o. Promoción o mantenimiento de actividades personales, o utilización de los recursos tecnológicos del Hospital Militar Central, para beneficio personal.

p. Uso de la identidad institucional digital (cuenta de usuario y contraseña) de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro funcionario.

q. Descuidar dejando al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del cumplimiento de sus funciones.

r. Retirar de las instalaciones del Hospital Militar Central, computadores de escritorio, portátiles e información física o digital clasificada, sin autorización o abandonarla en lugares públicos o de fácil acceso.

s. Entregar, enseñar y divulgar información clasificada del Hospital Militar Central, a personas o entidades no autorizadas.

t. Llevar a cabo actividades ilegales, o intentar acceso no autorizado a la plataforma tecnológica del Hospital Militar Central.

u. Ejecutar cualquier acción que difame, afecte la reputación o imagen del Hospital Militar Central, o alguno de sus funcionarios desde la Plataforma Tecnológica.

v. Realizar cambios no autorizados en la Plataforma Tecnológica del Hospital Militar Central.

w. Otorgar privilegios de acceso a los activos de información a funcionarios o terceros no autorizados.

x. Ejecutar acciones para eludir y/o modificar los controles establecidos en la presente directiva.

y. Consumir alimentos y bebidas, cerca de la plataforma tecnológica.

z. Conectar dispositivos diferentes a equipos de cómputo, a la corriente regulada.

aa. Realizar cualquier otra acción que contravenga disposiciones constitucionales, legales o institucionales.

La realización de alguna de estas prácticas u otras que afecten la seguridad de la información, acarrearán medidas administrativas, acciones disciplinarias y/o penales a que haya lugar, de acuerdo a los procedimientos establecidos para cada caso.

9. ORGANIZACIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACION DEL HOSPITAL MILITAR CENTRAL - *Ref: ISO/IEC 27001:2005 CL. A.6.1*

La estructura del comité de seguridad de la información del Hospital Militar Central deberá estar conformada por los siguientes actores:

a. Comité de Seguridad de la Información: El Comité deberá estar conformado mínimo por el jefe de la Unidad de Informática, el líder del área de seguridad de la información, el Oficial de Seguridad de la información, o quien haga sus veces para cada uno de los cargos anteriormente mencionados; un representante de control interno, un representante de la oficina jurídica y un representante de la oficina de seguridad.

b. El Comité de Seguridad de la información deberá realizar sesiones periódicas mínimo dos veces al año y cada vez que se requieran, la participación en estas sesiones es obligatoria para el Jefe de la Unidad de Informática, el líder del área de seguridad de la información, el Oficial de Seguridad, para el representante de la Oficina de Control Interno y, en los casos en que aplique el representante de la Oficina Asesora Jurídica y el representante de la Oficina de Seguridad.

Sus principales funciones serán:

1. Estructurar, evaluar y presentar estrategias y proyectos ante la alta dirección que permitan fortalecer la seguridad de la información del Hospital Militar Central.

2. Revisar en el marco de las sesiones ordinarias con frecuencia anual, o extraordinarias cuando las circunstancias así lo requieran, los aspectos relativos a las estrategias, protocolos y procedimientos aplicados o propuestos por sus integrantes en materia de seguridad de la información.

3. Gestionar las actividades de promoción y difusión de la cultura de seguridad de la información contenida en el presente documento.

4. Supervisar la gestión desarrollada por el líder del Grupo de Seguridad de la Información en la dirección del Sistema de Gestión de la Seguridad de la Información del Hospital Militar Central.

5. Gestionar la adquisición de soluciones o herramientas que apoyen la seguridad de la información y realizar el trámite ante el Comité de Integración de Tecnologías de la Información - CITI.

6. Estudiar y conceptuar sobre los casos especiales de seguridad de la información que se presenten y afecten al Hospital Militar Central, para recomendar las acciones pertinentes y apoyar la toma de decisiones.

7. Avalar los planes de pruebas y análisis de vulnerabilidades externas e internas a los componentes de la plataforma tecnológica, con el fin de garantizar un alto nivel de seguridad y que se cuente con las herramientas adecuadas para la protección de la misma.

8. Definir el estándar para realizar el levantamiento del inventario de activos de información, la clasificación y la rotulación de los mismos, de acuerdo con su nivel de confidencialidad y criticidad.

9. Establecer la metodología para el análisis de riesgos, donde se identifiquen los activos de información críticos, su impacto, las amenazas, vulnerabilidades y probabilidad de ocurrencia, y se establezcan las respuestas necesarias para su tratamiento.

10. Mantener actualizada las políticas y procedimientos del Sistema de Gestión de Seguridad de la Información de acuerdo a la estrategia sectorial del Ministerio de Defensa Nacional.

11. Reportar al Comité de Seguridad de la Información Sectorial aquellos casos que requieran de su intervención.

c. Líder del Área de Seguridad de la Información: para este rol será designado un funcionario del Hospital Militar Central y será el responsable por la definición, implementación, operación, mantenimiento y mejoramiento del Sistema de Gestión de Seguridad de la Información.

Perfil: Ingeniero de sistemas, electrónico o afines, mínimo con especialización en seguridad informática o de la información.

Sus principales funciones serán:

1. Ejecutar las tareas de seguridad de la información que le asigne el Comité de Seguridad de la Información.

2. Mantener informado al Comité de Seguridad de la Información, sobre los eventos e incidentes de seguridad que se presenten al interior de la misma.

3. Gestionar la actualización del Sistema de Gestión de Seguridad de la Información.

4. Definir la estrategia de gestión de los riesgos de seguridad de la información, coordinar su implementación y centralizar el monitoreo sobre su ejecución.

5. Definir, documentar, mantener, divulgar y actualizar los procedimientos propios de la gestión del Sistema de Gestión de Seguridad de la Información.

6. Supervisar el cumplimiento de los procedimientos del Sistema de Gestión de Seguridad de la Información.

7. Promover la creación y actualización de las políticas y estándares de seguridad de la información y velar por el cumplimiento de las mismas.

8. Apoyar la consolidación de la cultura de seguridad de la información entre todo el personal.

9. Coordinar la difusión de cualquier comunicación relacionada con el Comité de Seguridad de la Información.

10. Participar activamente en las actividades convocadas por el Comité de Seguridad de la Información.

11. Coordinar la realización periódica de auditorías internas y pruebas de vulnerabilidad de acuerdo con las políticas establecidas, previa autorización del Comité de Seguridad de la Información.

12. Elaborar y proponer al Comité de Seguridad de la Información, planes, procedimientos y controles para el mejoramiento del Sistema de Gestión de Seguridad de la Información.

13. Proponer al Comité de Seguridad de la Información, planes de capacitación, concientización y entrenamiento para difundir las políticas, normas y estándares de seguridad de la información al personal.

14. Apoyar y coordinar el desarrollo de actividades de investigación y búsqueda de información referente a seguridad de la información.

15. Elaborar los informes que le sean requeridos por el Comité de Seguridad de la Información sobre el Sistema de Gestión de Seguridad de la Información de la dependencia o entidad.

16. Coordinar la implementación de acciones preventivas y correctivas del Sistema de Gestión de Seguridad de la Información con los respectivos responsables, de acuerdo con los resultados de las auditorías internas o externas.

17. Implementar y hacer seguimiento al plan de mejora continua del Sistema de Gestión de Seguridad de la Información.

18. Liderar el proceso de certificación y recertificación.

19. Proponer y apoyar proyectos de seguridad de la información.

d. Oficial o promotor de Seguridad de la Información: para este rol será designado un funcionario del Hospital Militar Central y será el apoyo para el Jefe de la Unidad de Informática en la implementación de las actividades y controles necesarios para llevar a cabo el desarrollo del Sistema de Gestión de Seguridad de la Información.

Perfil: Técnico, tecnólogo ó ingeniero, en el área de sistemas, electrónica o afines, con capacitación básica en seguridad de la información y/o en la norma ISO 27000.

Sus principales funciones serán:

1. Desarrollar campañas de sensibilización y concientización que garanticen el fortalecimiento de la cultura de seguridad de la información entre todos los funcionarios.

2. Velar por la difusión y cumplimiento de las políticas y estándares de Sistema de Gestión de Seguridad de la Información.

3. Asesorar y recomendar al líder de Seguridad de la Información y dueños de procesos en temas relacionados con la Seguridad de la Información.

4. Apoyar al jefe de la Unidad de informática, en la implementación técnica y operativa de controles de seguridad de la información pertinentes al proceso del Sistema de Gestión de Seguridad de la Información.

5. Apoyar a las áreas de tecnología en el proceso de análisis y evaluación de riesgos.

6. Realizar la gestión de incidentes de seguridad y reportarlos al líder de Seguridad de la Información.

7. Apoyar al Líder del Área de Seguridad de la Información durante la ejecución de las auditorías internas o externas al Sistema de Gestión de Seguridad de la Información.

8. Será el responsable de evaluar y autorizar las solicitudes de conexiones remotas y demás acceso externos a la plataforma tecnológica del Hospital Militar Central.

10. REVISION INDEPENDIENTE – AUDITORIAS INTERNAS - Ref: ISO/IEC 27001:2005 CL. A.6.1.8.

Se deberán realizar revisiones periódicas al Sistema de Gestión de Seguridad de la Información, según el procedimiento de Auditorías Internas (Anexo R) , para verificar su vigencia, su correcto funcionamiento y su efectividad.

11. GESTION DE TERCEROS - *Ref: ISO/IEC 27001:2005 CL A.6.2.2*

a. Cuando exista la necesidad de otorgar acceso a terceras partes a la plataforma tecnológica del Hospital Militar Central, el Oficial de Seguridad de la Información y el propietario de la información que se trate llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta entre otros los siguientes aspectos:
   - El tipo de acceso requerido (físico, lógico y a qué recurso)
   - Los motivos para los cuales solicita el acceso
   - El valor de la información
   - Los controles empleados por la tercera parte
   - La incidencia de este acceso en la seguridad de la información de las dependencias o entidades

b. En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de las instalaciones del Hospital Militar Central se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

c. En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que definan las condiciones para la conexión o el acceso.

d. El acceso de los terceros a la información o a cualquier elemento de la infraestructura tecnológica, así como las modificaciones sesiones o terminaciones de las obligaciones contractuales y/o actividades, debe ser solicitado por el supervisor o persona a cargo del tercero al propietario de dicho activo quien, en conjunto con el Oficial de Seguridad de la Información, aprobarán y autorizarán el acceso y uso de la información.

e. Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de computadores, contemplarán como mínimo los siguientes aspectos:

   - Forma en los que se cumplirán los requisitos legales aplicables
   - Medios para garantizar que todas las partes involucradas en la tercerización incluyendo los subcontratistas, conocen sus responsabilidades en materia de seguridad.
   - Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos

- Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible
- Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
- Niveles de seguridad física que se asignará al equipamiento tercerizado.
- Derecho a la auditoría por parte del Hospital Militar Central.

11.1 Acuerdos de Confidencialidad - *Ref.: ISO/IEC 27001:2005 CL. A.6.1.*

Todos los funcionarios, contratistas y demás terceros deben firmar la cláusula y/o acuerdo de confidencialidad y este deberá ser parte integral de los contratos utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada, de acuerdo a formato de confidencialidad. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos a personas o entidades externas.

11.2 Acuerdos de Intercambio de Información y Software

a. Todo funcionario, contratista o terceras personas del Hospital Militar Central son responsables por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

b. Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad de acuerdo a la reglamentación vigente.

c. El intercambio de información y software con otras entidades, se realiza previa celebración de convenio interadministrativo en el que se establecen cláusulas de responsabilidad, deberes y derechos.

d. En todo caso, estos acuerdos deben velar por el cumplimiento de las regulaciones legales, propiedad intelectual y protección de datos personales. Así mismo se especifican las consideraciones de seguridad y

reserva de la información y las responsabilidades por el mal uso o divulgación de la misma.

e. Cuando la información sea solicitada por autoridad judicial o administrativa competente; la entrega se realiza siguiendo el procedimiento establecido.

f. El intercambio de información contempla las siguientes directrices:

- Uso de web services, para la publicación y consumo de información electrónica.
- Uso de canales cifrados.
- Respeto por los derechos de autor del software intercambiado, por tratarse de un bien fiscal de la entidad.
- Términos y condiciones de la licencia bajo la cual se suministra el software.
- Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendida por el receptor de la información.
- Informar al titular de los datos, el intercambio de estos con otras entidades.
- Informar sobre la propiedad de la información suministrada y las condiciones de su uso.

12. GESTION DE ACTIVOS DE INFORMACION - *Ref.: ISO/IEC 27001:2005 CL. A.7.1.1. y CL. A.7.1.2.*

a. El Hospital Militar Central será responsable la custodia sobre todo dato, información y mensaje generado, procesado y contenido por sus sistemas de cómputo, así como también de todo aquello transmitido a través de su red de telecomunicaciones o cualquier otro medio de comunicación físico o electrónico y se reserva el derecho de conceder el acceso a la información.

b. El Hospital Militar Central deberá identificar los activos asociados a cada sistema de información, sus respectivos propietarios y su ubicación a fin de elaborar y mantener un inventario actualizado de los activos de información, de acuerdo al procedimiento de Inventario y Clasificación de Activos de Información.

c. El Hospital Militar Central deberá realizar la clasificación y control de activos con el objetivo de garantizar que los activos de información reciban un apropiado nivel de

protección, clasificar la información para señalar su sensibilidad y criticidad y definir los niveles de protección y medidas de tratamiento de acuerdo al procedimiento de Inventario y Clasificación de Activos de Información.

d. El Hospital Militar Central deberá realizar la clasificación de la información, evaluando las tres características de la información en las cuales se basa la seguridad de la información: confidencialidad, integridad y disponibilidad.

e. El Hospital Militar Central deberá definir procedimientos para el rotulado y manejo de información de acuerdo al esquema de clasificación definido.

13. USO ADECUADO DE LOS ACTIVOS DE INFORMACION- *Ref.: ISO/IEC 27001:2005 CL. A.7.1.3*

La información, los sistemas, las aplicaciones, los servicios y los equipos (equipos de escritorio, portátiles, impresoras, redes, Internet, dispositivos móviles, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) del Hospital Militar Central, son activos de información que se proporcionan a los funcionarios, contratistas y demás terceros autorizados para cumplir con actividades laborales.

El Hospital Militar Central se reserva el derecho de monitorear y supervisar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en esta política y la legislación vigente.

13.1 Uso de Internet

Internet es una herramienta de trabajo que permite navegar en sitios relacionados o no con las actividades diarias, por lo cual el uso adecuado de este recurso se controla, verifica y monitorea, considerando para todos los casos, las siguientes políticas:

a. La navegación en Internet estará controlada de acuerdo con las categorías de navegación definidas para los usuarios; sin embargo, en ningún caso se considerarán aceptables los siguientes usos:

   1. Navegación en sitio de contenido sexualmente explícito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.

   2. Publicación, envío o adquisición de material sexualmente explícito, discriminatorio, que implique un delito informático o de

cualquier otro contenido que se considere fuera de los límites permitidos.

3. Publicación o envío de información confidencial hacia afuera de las dependencias y entidades del Sector Defensa sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.

4. Utilización de otros servicios disponibles a través de Internet que permitan establecer conexiones o intercambios no autorizados por el oficial de seguridad o quien haga sus veces.

5. Publicación de anuncios comerciales o material publicitario, salvo las oficinas que dentro de sus funciones así lo requieran. Estas solicitudes, deben ser justificadas por el jefe de la oficina y avaladas por el oficial de seguridad de la información o quien haga sus veces.

6. Promover o mantener asuntos o negocios personales.

7. Utilización de programas de aplicación o software no relacionados con la actividad laboral y que afecte el procesamiento de la estación de trabajo o de la red.

8. Navegación en las cuentas de correo de carácter personal, no institucional, o en redes sociales, sin una justificación de negocio por parte de la Entidad.

9. Uso de herramientas de mensajería instantánea no autorizadas por el área o grupo de Seguridad de la Información.

10. Emplear cuentas de correo externas no corporativas para el envío o recepción de información institucional.

b. Se realizará monitoreo permanente de tiempos de navegación y páginas visitadas por los funcionarios, contratistas y demás terceros autorizados. Así mismo, se puede inspeccionar, registrar e informar las actividades realizadas durante la navegación.

c. Cada uno de los usuarios es responsable de dar un uso adecuado de este recurso y en ningún momento puede ser empleado para realizar prácticas ilícitas o mal

intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información de la Entidad, entre otros.

d. Los funcionarios, contratistas y demás terceros no pueden asumir en nombre del Hospital Militar Central conceptos personales en encuestas de opinión, foros u otros medios similares.

e. El uso de Internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información.

13.2 Uso del correo electrónico

La asignación de una cuenta de correo electrónico corporativo se da como herramienta de trabajo para cada uno de los funcionarios que la requieran para el desempeño de sus funciones, así como a contratistas y otros terceros previa autorización; su uso se encuentra sujeto a las siguientes reglas:

a. La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de cada una de las entidades y dependencias que conforman el Sector Defensa.

b. Los mensajes y la información contenida en los buzones de correo son de propiedad del Hospital Militar Central y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones. Por este motivo la información y tráfico de la misma se considera de interés del Hospital Militar Central.

c. El tamaño de los buzones y mensajes de correo será determinado por la Unidad de Informática, conforme a las necesidades de cada usuario y previa autorización del Jefe inmediato.

d. No se considera aceptado el uso del correo electrónico corporativo para los siguientes fines:

1. Enviar o retransmitir cadenas de correo, mensajes con contenido racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.

2. Enviar mensajes no autorizados con contenido religioso o político.

3. El envío de archivos adjuntos con extensiones como .mp3, .wav, .exe, .com, .dll, .bat, .msi o cualquier otro archivo que ponga en riesgo la seguridad de la información; en caso que sea necesario hacer un envío de este tipo de archivos deberá ser autorizado por el Oficial de Seguridad de la Información o quien haga sus veces.

4. El envió de información relacionada con la defensa y la seguridad nacional a otros dominios diferentes al de cada una de las entidades y dependencias que conforman el Sector Defensa, sin la autorización previa del oficial de Seguridad de la Información y el respectivo propietario de la información o quien haga sus veces.

5. El envío masivo de mensajes corporativos deberá ser solicitado por el Jefe de la Dependencia que lo requiere y contar con la aprobación de la respectiva Oficina de Tecnología o quien tenga a cargo dicha función.

e. Toda información generada que requiera ser transmitida fuera del Hospital Militar Central, y que por sus características de confidencialidad e integridad debe ser protegida, debe estar en formatos no editables y con mecanismos de seguridad. Sólo puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

f. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido y deben conservar, en todos los casos, el mensaje legal institucional de confidencialidad.

g. Todo correo electrónico deberá tener al final del mensaje un texto en español e inglés en el que se contemplen, mínimo, los siguientes elementos:

1. El mensaje (incluyendo cualquier anexo) contiene información confidencial y se encuentra protegido por la Ley.

2. El mensaje sólo puede ser utilizado por la persona o empresa a la cual está dirigido.

3. En caso de que el mensaje sea recibido por alguna persona o empresa no autorizada, solicitar borrarlo de forma inmediata.

4. Prohibir la retención, difusión, distribución, copia o toma de cualquier acción basada en el mensaje.

13.3 Uso de Redes Inalámbricas

a. Se debe propender por la implementación de ambientes de trabajo completamente independientes para la red operativa y la red con servicio de internet a fin de minimizar los riesgos de intrusión a las redes institucionales.

b. Los usuarios de las redes inalámbricas deben ser sometidos a las mismas condiciones de seguridad de las redes cableadas en lo que respecta identificación, autenticación, control de contenido de internet y cifrado entre otros.

c. El Oficial de Seguridad de la Información o el que haga sus veces será el responsable de validar a quien se le serán asignados los servicios a través de redes inalámbricas.

d. El servicio de Internet en las áreas de bienestar y capacitación así como de investigación, deberá contar con mecanismos de autenticación de usuarios y deberá estar configurado de tal manera que permita el desarrollo de las actividades académicas y de investigación.

e. El servicio de Internet en las áreas destinadas para el bienestar social, deberá contar con mecanismos de autenticación de usuarios y deberá estar configurado de tal manera que garantice bienestar.

f. El servicio de internet en las áreas de capacitación y en las instalaciones destinadas para el bienestar social, deben estar configuradas de forma independiente a la red operativa de la dependencia o entidad del Sector Defensa.

g. Se deben implementar equipos inalámbricos que permitan configuraciones de seguridad (hardening). En ningún caso se podrá dejar configuraciones y contraseñas por defecto.

13.4 Segregación de Redes

a. La plataforma tecnológica del Hospital Militar Central que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet.

b. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere.

c. La Unidad de Informatica, es la encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

13.5 Uso de Computación en la Nube (Cloud Computing)

a. Por ningún motivo se podrá almacenar información clasificada en servicios en la nube (Cloud Computing) públicos o híbridos.

b. Ningún servicio de carácter operativo e institucional de las dependencias o entidades del Sector Defensa, deberán ser contratados en Servicios en la Nube (Cloud Computing) públicos o híbridos.

c. Para el caso de las escuelas de formación y capacitación se podrá hacer uso de servicios en la nube (Cloud Computing) públicos e híbridos, siempre y cuando no se vea comprometida la seguridad institucional o información clasificada.

d. El Hospital Militar Central, podrá implementar servicios en la nube (Cloud Computing) privado, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de los controles adecuados.

13.6 Sistemas de Acceso Público

a. La información pública producida por el Hospital Militar Central, deberá estar resguardada de posibles modificaciones que afecten la imagen institucional.

b. El portal institucional, deberá contener la política de privacidad y uso, así como la política de seguridad del mismo.

c. La Unidad de Informática deberá garantizar al público que hace uso de los servicios del portal institucional, el derecho de Habeas Data y propende por la seguridad de la información de terceros depositada en custodia, pero no es responsable de la veracidad de la misma.

d. Toda la información publicada en el portal institucional o cualquier otro medio, deberá contar con la revisión y aprobación del área de Comunicaciones y deberá estar debidamente rotulada, según su nivel de clasificación.

13.7 Uso de recursos tecnológicos

La asignación de los diferentes recursos tecnológicos se da como herramientas de trabajo para uso exclusivo de los funcionarios, contratistas y demás terceros autorizados. El uso adecuado de estos recursos se encuentra sujeto a las siguientes reglas:

a. La instalación de cualquier tipo de software en los equipos de cómputo del Hospital Militar Central es responsabilidad exclusiva de la Unidad de Informática, por tanto son los únicos autorizados para realizar esta labor.

b. Ningún activo de información adquirido y que sea configurable, debe ser instalado con la configuración por defecto del fabricante o proveedor, incluyendo cuentas y claves de administrador.

c. Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla no definido. Estos cambios pueden ser realizados únicamente por la Unidad de Informática.

d. Los equipos de cómputo deberán ser bloqueados, por los usuarios que los tienen a cargo, cada vez que se retiren del puesto de trabajo.

e. Los requerimientos de recursos tecnológicos de los usuarios del Hospital Militar Central deberán ser avalados por la Unidad de Informática.

f. Los usuarios no deben realizar cambios físicos en las estaciones de trabajo, tales como, cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física. Estas actividades sólo podrán ser realizadas por la Unidad de Informática.

g. Los recursos tecnológicos asignados a los funcionarios, contratistas y demás terceros autorizados tienen el único propósito de contribuir a la realización de sus actividades laborales e institucionales.

h. Los equipos de cómputo asignados, deben ser devueltos a la dependencia responsable una vez sean reemplazados o cuando el funcionario o contratista responsable de dicho equipo finalice su vinculación con el Hospital Militar Central.

i. De acuerdo con el literal anterior, las dependencias no deben almacenar equipos de cómputo en las oficinas una vez haya cesado el uso de los mismos.

13.8 Seguridad de los Activos Informáticos - *Ref.: ISO/IEC 27002*

Con el fin de evitar la pérdida, daño, robo o puesta en peligro de los activos y a su vez la interrupción de las actividades del Hospital Militar Central, los equipos deberán estar protegidos contra amenazas físicas y ambientales, para lo anterior se definen las siguientes directrices que regularan el uso de los activos informáticos dentro y fuera de las instalaciones del Hospital Militar Central:

a. No se deberán ubicar activos informáticos en áreas comunes o de acceso público sin la debida protección aprobada por el oficial de seguridad.

b. No se deberán crear ubicaciones compartidas ni servicios de almacenamiento de datos diferentes a los provistos por la Unidad de Informatica del Hospital Militar Central o los aprobados por el comité de seguridad informatica, así mismo la Unidad de Informatica es responsable de la custodia y disponibilidad de esta información.

c. Está prohibido comer, beber, fumar cerca de cualquier activo informático del Hospital Militar Central.

d. Todos los usuarios del Hospital Militar Central que hagan uso de los activos informáticos deberán reportar a la Unidad de informatica cualquier novedad o amenaza física (robo, incendio, explosión, humo, agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética o vandalismo) que afecten la integridad de los activos informáticos.

e. La unidad de informatica deberá monitorear las variables ambientales como humedad y temperatura del centro de datos con el fin de determinar las condiciones adversas que podrían afectar adversamente el funcionamiento de los servicios de procesamiento de información.

f. Todos los usuarios del Hospital Militar Central, deberán dar buen uso de los activos informáticos, en caso de encontrar alguna anomalía en uno de ellos esta deberá ser reportada a la Unidad de informatica.

14 CLASIFICACION DE LA INFORMACION - *Ref: ISO/IEC 27001:2005 CL. A.7.2.*

a. Toda la información deberá ser identificada, clasificada y documentada con base en 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:*** *La información se clasificará según su confidencialidad de la siguiente manera:*

1. **Ultrasecreto**: 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.

2. **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.

4. **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.

5. **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:** La información se clasificará según su integridad de la siguiente manera:

1. No puede repararse y ocasiona pérdidas graves para el país.
2. No puede repararse y ocasiona pérdidas graves para la institución.
3. Difícil reparación y pérdidas significativas.

4. Puede repararse, pérdidas leves.
5. No afecta la operación y puede repararse fácilmente.

- **Según su disponibilidad:** La información se clasificará según su disponibilidad de la siguiente manera:

  Es necesario determinar el tiempo máximo tolerable MTD de indisponibilidad que puede soportar el área y/o la entidad sin un activo determinado, para lo cual se tendrá en cuenta la siguiente clasificación:

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

b. Toda información que no corresponda a alguno de los niveles de clasificación mencionados anteriormente se considerará pública.

c. Los propietarios de los activos de información son los responsables de establecer el nivel de clasificación de cada activo.

15 ANALISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACION

a. El Hospital Militar Central, deberá realizar el análisis y evaluación de riesgos como base para identificar y tasar los riesgos de seguridad de la información a los cuales están expuestos los activos de información, con el objetivo de definir e implementar las opciones de tratamiento apropiadas.

b. Para la valoración de activos de información y sus riesgos asociados se empleará una metodología basada en la norma ISO/IEC 27005:2008, la cual contiene las siguientes actividades generales:

1. Identificación de activos de información.
2. Valoración del impacto de los activos de información.
3. Identificación de escenarios de riesgo basados en las amenazas y vulnerabilidades posibles.
4. Valoración de la probabilidad de ocurrencia de los escenarios de riesgo.
5. Valoración de la efectividad de los controles implementados.
6. Cálculo del nivel de riesgo de seguridad de la información.

7. Identificación de opciones para el tratamiento de los riesgos que sean valorados en un nivel no aceptable.

c. Las actividades necesarias para ejecutar el análisis de riesgos se realizan de acuerdo con el siguiente esquema:

1. Definición de los procesos críticos a los cuales se les aplicará el análisis de riesgos.
2. Entrevistas con los responsables de los activos con el fin de dar a conocer la metodología y hacer el levantamiento de activos de información.
3. Análisis y evaluación de los riesgos de seguridad de la información para los activos que soportan los procesos críticos.
4. Identificación de opciones de tratamiento de riesgos (Anexo S)
5. Comunicación de resultados al Comité de Seguridad de la Información.

d. 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 Sector Defensa, en la plataforma tecnológica, en los procesos, entre otros.

16 CONCIENTIZACION Y CAPACITACION EN SEGURIDAD DE LA INFORMACION - *Ref: ISO/IEC 27001:2005 CL. A.8.2.2*

a. El Hospital Militar Central, deberá mantener un programa anual de concientización y capacitación para todos sus funcionarios, así como para los contratistas y terceros que interactúen con la información institucional y desarrollen actividades en sus instalaciones. Esto con el fin de proteger la información y la infraestructura tecnológica que la soporta.

b. Todos los funcionarios, contratistas y demás terceros al servicio del Hospital Militar Central, deben ser informados y capacitados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas.

17 FINALIZACION DE LA RELACION LABORAL - *Ref: ISO/IEC 27001:2005 CL. A.8.3.*

a. En el momento de la desvinculación o de cambio de roles en el Hospital Militar Central, todo funcionario, contratista y/o tercero debe hacer entrega de todos los activos de información que le hayan sido asignados mediante el formato establecido.

18 SEGURIDAD FISICA Y AMBIENTAL - *Ref: ISO/IEC 27001:2005 CL. A.9*

a. La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas, alrededor de las instalaciones del Hospital Militar Central.

b. Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el oficial de seguridad de la información, a fin de permitir el acceso solo a personal autorizado.

c. Para la selección de las áreas protegidas se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil y otras formas de desastres naturales o provocados por el hombre. También se tomaran en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad.

d. Para incrementar la seguridad de las áreas protegidas se establecerán controles y lineamientos adicionales, que incluyan controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí.

e. Las plataformas tecnológicas serán ubicadas y protegidas de tal manera que reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.

f. El cableado de energía eléctrica y comunicaciones que transportan datos o brindan apoyo a los servicios de información estarán protegidos contra intercepción o daños.

g. El Hospital Militar Central, deberá acoger los lineamientos a que haya lugar de acuerdo a la normatividad ambiental vigente para el Manejo de Residuos de Aparatos Eléctricos y Electrónicos (RAEE), de tal forma que se busque la prevención y reducción de los impactos ambientales.

h. Se deberá garantizar la seguridad física del Centro de Datos, incluyendo entre otros los siguientes subsistemas:

   a. Sistema Eléctrico
   b. Sistema de protección contra incendios
   c. Control de temperatura

18.1 Acceso Físico - *Ref: ISO/IEC 27001:2005 CL. A.9.1.*

La seguridad física es importante para el cuidado y protección de la información, por esto se han definido las siguientes reglas:

a. El área de seguridad de la información en coordinación con el área de seguridad, evaluarán las necesidades de capacitación e implementación de los procedimientos y controles necesarios para garantizar la integridad, disponibilidad y confidencialidad de los activos de información.

b. Todas las puertas que utilicen sistema de control de acceso, deberán permanecer cerradas, y es responsabilidad de todos los funcionarios, contratistas y demás terceros autorizados evitar que las puertas se dejen abiertas.

c. Se debe exigir a todo el personal, sin excepción, el porte en un lugar visible del mecanismo de identificación.

d. Los visitantes deberán permanecer acompañados de un funcionario cuando se encuentren dentro de alguna de las áreas seguras.

e. Es responsabilidad de todos los funcionarios, contratistas y demás terceros borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo y garantizar que no queden documentos o notas escritas sobre las mesas.

f. Es responsabilidad de todos los funcionarios, contratistas y demás terceros acatar las normas de seguridad y mecanismos de control de acceso a las instalaciones del Hospital Militar Central.

g. Los funcionarios, contratistas y demás terceros, así como los visitantes, deberán tener acceso físico restringido a los sitios que requieran y les sean autorizados para el cumplimiento de sus funciones, tareas o misión dentro de las instalaciones.

18.2 Trabajo en Áreas Protegidas - *Ref: ISO/IEC 27001:2005 CL. A.9.1.5.*

a. Todas las áreas que se hayan definido como protegidas y activos de información que la componen mediante el procedimiento de control de acceso a área protegida, son considerados áreas seguras; por lo tanto deben ser protegidos de acceso no autorizado mediante controles y tecnologías de autenticación.

b. Todo acceso físico a las áreas protegidas deberá estar manejado según los lineamientos definidos por el procedimiento de Control de Acceso a Área protegida.

c. En las áreas seguras donde se encuentren activos informáticos, se debe cumplir como mínimo con los siguientes lineamientos:

1. No se deben consumir alimentos ni bebidas.
2. No se deben ingresar elementos inflamables.
3. No se debe permitir el acceso de personal ajeno sin que este acompañado por un funcionario durante el tiempo que dure su visita.
4. No se deben almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.
5. No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.
6. No se permite el ingreso de equipos electrónicos, así como maletas o contenedores, a menos que haya una justificación para esto. En ese caso, deberán ser registradas al ingreso y salida para minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de elementos.

d. Las áreas protegidas deben contar con las condiciones ambientales que garanticen la correcta operación de los equipos y el estado de los medios que contienen información, así como un sistema de detección y control de incendios.

19 SEGURIDAD Y MANTENIMIENTO DE LOS EQUIPOS - *Ref: ISO/IEC 27001:2005 CL. A.9.2.*

a. Los equipos que hacen parte de la infraestructura tecnológica del Hospital Militar Central deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.

b. El Hospital Militar Central adoptará los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo entre otros.

c. Los funcionarios, al igual que los contratistas y demás terceros que tengan acceso a los equipos que componen la infraestructura tecnológica no deben comer, fumar, beber o consumir algún tipo de alimento cerca de los equipos.

d. Los funcionarios, contratistas y demás terceros velarán por el uso adecuado de los equipos de escritorio, portátiles y móviles que les hayan sido asignados, por lo

tanto, dichos equipos no deberán ser prestados a personas ajenas o no autorizadas.

e. El Hospital Militar Central deberá proveer los suministros y equipamiento de soporte para los sistemas y plataforma tecnológica tales como: electricidad, agua, aire acondicionado, planta eléctrica y un sistema de alimentación eléctrica no interrumpida (UPS), entre otros. Estos suministros deben ser monitoreados, revisados y medidos regularmente para asegurar su funcionamiento bajo condiciones normales y evitar futuros daños.

f. La Unidad de Informática, deberá realizar el mantenimiento a los equipos de cómputo, servidores, equipos portátiles y equipos periféricos dentro de las instalaciones del Hospital Militar Central, el cual debe ser programado periódicamente bajo un cronograma anual de mantenimiento.

g. Se debe asegurar que, sobre la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, se realicen mantenimientos periódicos con el fin de que dichas actividades no se vean afectadas por obsolescencia. Por lo tanto, revisará constantemente la vida útil de cada uno de los recursos que componen dicha infraestructura de acuerdo con la descripción y recomendaciones de sus fabricantes.

h. Los equipos tales como máquinas de copiado, impresoras y máquinas de fax deberán estar ubicados en zonas de acceso restringido y se permitirá el uso únicamente a personal autorizado.

i. Los equipos portátiles deberán estar asegurados (cuando estén desatendidos) con la guaya o el mecanismo que se defina para su protección, sea dentro o fuera de las instalaciones del Hospital Militar Central.

j. El Hospital Militar Central garantizará la existencia de pólizas o seguros para la reposición de los activos informáticos que respaldan los planes de contingencia y la continuidad de los servicios.

20 SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES - *Ref: ISO/IEC 27001:2005 CL. A.9.2.5.*

a. Los usuarios que requieran manipular los equipos o medios fuera de las instalaciones del Hospital Militar Central, deben velar por la protección de los mismos sin dejarlos desatendidos en lugares públicos o privados en los que se puedan ver comprometidos la imagen o información de la entidad.

b. El propietario del activo en coordinación con el Oficial de Seguridad de la Información (o quién haga sus veces) identificará los riesgos potenciales que puede generar el retiro de equipos o medios de las instalaciones mediante la metodología de análisis de riesgos establecida; así mismo, establecerá los controles necesarios para la mitigación de dichos riesgos.

c. En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información relacionada con la entidad, se deberá realizar inmediatamente el respectivo reporte de acuerdo con el procedimiento Gestión de Incidentes de seguridad y se deberá poner la denuncia ante la autoridad competente, se enviará reporte a la Oficina de Control Interno Disciplinario, para que inicien las investigaciones correspondientes.

d. Los equipos de cómputo o activos de información que por razones del servicio se retiren de las instalaciones del Hospital Militar Central, deberán contener únicamente la información estrictamente necesaria para el cumplimiento de su misión y se deshabilitarán los recursos que no se requieren o puedan poner en riesgo la información que contiene.

21 TRASLADO DE PROPIEDAD - *Ref: ISO/IEC 27001:2005 CL. A.9.2.7.*

a. El retiro de equipos o medios que procesan o almacenan algún tipo de información y/o que hacen parte de la plataforma tecnológica, debe ser autorizado por el propietario del activo previa solicitud del funcionario interesado. Si el activo está clasificado como relacionado con la seguridad de la información, el retiro deberá estar autorizado también por el Ayudante General (o quién haga sus veces).

b. Todo el personal que por cumplimiento de sus funciones institucionales necesite retirar un equipo, medio de almacenamiento, información o software de las instalaciones del Hospital Militar Central, deben ser debidamente identificados y registrados antes de conceder la autorización respectiva.

c. El Hospital Militar Central proporcionará los mecanismos y recursos necesarios para que en cada punto de acceso a las instalaciones exista un puesto de revisión donde se inspeccione y se lleve el control de los equipos que son ingresados y retirados.

d. Los equipos de contratistas y demás terceros que hayan sido autorizados para acceder a la redes de datos sólo podrán ser retirados al finalizar el contrato o las labores para las cuales estaba definido, previo borrado seguro de la información a

través del proceso de sanitización. La Unidad de Informática, generará un paz y salvo como constancia de dicho proceso, que deberá ser presentado al momento del retiro del equipo de las instalaciones físicas correspondientes.

22 DOCUMENTACION DE PROCEDIMIENTOS OPERATIVOS - *Ref: ISO/IEC 27001:2005 CL. A.10.1*

a. La ejecución de cualquier actividad asociada con la infraestructura tecnológica para el procesamiento de información, comunicaciones y seguridad informática debe estar soportada por instrucciones o procedimientos operativos documentados, los cuales siempre deben estar a disposición de todos los usuarios que los necesiten para el desarrollo de sus labores.

b. Los procedimientos operativos deben quedar documentados con instrucciones detalladas, teniendo en cuenta el procesamiento y manejo de información, instrucciones para el manejo de errores, contactos de soporte en caso de dificultades técnicas u operativas inesperadas, así como instrucciones para el manejo de medios y exposición de resultados especiales y de carácter confidencial.

c. La elaboración, publicación y modificación que se realice de los documentos debe ser autorizada por el administrador de la aplicación, propietario del activo, Jefe de dependencia o el funcionario a quien se le hayan otorgado dichas funciones.

d. Los procedimientos operativos deben contener instrucciones para el manejo de errores que se puedan presentar en la ejecución de las actividades, contactos de soporte, procedimientos de reinicio y recuperación de sistemas y aplicaciones, forma de procesamiento y manejo de la información, copia de respaldo de la información y los demás a los que hubiere lugar.

23 CONTROL DE CAMBIOS OPERATIVOS - *Ref: ISO/IEC 27001:2005 CL. A.10.1.2.*

a. Todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica debe ser controlado, gestionado y autorizado adecuadamente por parte de la Unidad de Informática, y debe cumplir con una planificación y ejecución de pruebas que identifiquen riesgos e impactos potenciales asociados que puedan afectar su operación.

b. Todos los cambios que se realicen sobre los sistemas de información y la infraestructura tecnológica deberán estar precedidas de la definición de los requerimientos, especificaciones y controles definidos en el procedimiento de

Control de Cambios. Dicha definición deberá ser realizada teniendo en cuenta como mínimo la confidencialidad, integridad y disponibilidad de la información.

24 SEGREGACION DE FUNCIONES - *Ref: ISO/IEC 27001:2005 CL. A.10.1.3.*

a. Todas las personas que tengan acceso a la infraestructura tecnológica o a los sistemas de información, deben contar con una definición clara de los roles y funciones sobre estos para reducir y evitar el uso no autorizado o modificación no intencional sobre los activos de información. Esta definición de segregación de funciones debe estar previamente aprobada por el jefe de la Unidad de Informática en coordinación con el Jefe de área de la dependencia.

b. La segregación de funciones sobre la infraestructura tecnológica y sobre los sistemas de información deberá ser revisada periódicamente por la Unidad de Informática con el fin de mantener actualizada dicha información y acorde con la realidad de la entidad.

25 SEPARACION DE AMBIENTES - *Ref: ISO/IEC 27001:2005 CL. A.10.1.4.*

a. El Hospital Militar Central proveerá los mecanismos, controles y recursos necesarios para contar con niveles adecuados de separación lógica y/o física entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica y sistemas de información, con el fin de reducir el acceso no autorizado y evitar cambios que pudieran afectar su operación.

b. El paso de software y hardware de un ambiente a otro deberá ser controlado y gestionado, de acuerdo con lo definido en el Procedimiento de Control de cambios.

c. Los usuarios deberán utilizar diferentes perfiles para el ambiente de desarrollo, de pruebas y de producción; así mismo, se deberá asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente para el desarrollo de sus funciones.

d. No deberán realizarse pruebas, instalaciones o desarrollos de hardware o software directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad o confidencialidad de la información.

e. El ambiente del sistema de prueba debe emular el ambiente de producción lo más estrechamente posible.

f. No se permite la copia de información Ultra Secreta, Secreta, Reservada, Confidencial, Restringida o Exclusiva de comando, desde el ambiente de producción al ambiente de pruebas; en caso de que sea estrictamente necesario, la copia debe ser autorizada por el propietario de la información y el Oficial de Seguridad de la Información y se deben implementar controles que garanticen que la confidencialidad de la información sea protegida y se elimine de forma segura después de su uso.

g. Se restringe el acceso a los compiladores, editores, utilidades de los sistemas y otras herramientas de desarrollo desde los sistemas del ambiente de producción y a cualquier usuario que no lo requiera para el desarrollo de su labor.

h. Periódicamente se podrá verificar las versiones instaladas tanto en ambiente de pruebas como en producción y confrontará esta información con revisiones previas y con las versiones de programas fuentes almacenadas en los repositorios del Hospital Militar Central.

26 GESTION DE LA CAPACIDAD - *Ref: ISO/IEC 27001:2005 CL. A.10.3.1.*

a. La Unidad de Informática, como área responsable de la administración de la plataforma tecnológica, deberá implementar los mecanismos, controles y herramientas necesarias para asegurar que los recursos que componen dicha plataforma sean periódicamente monitoreados, afinados y proyectados para futuros requerimientos de capacidad de procesamiento y comunicación, conforme a lo establecido en el Procedimiento Gestión de la Capacidad.

b. El responsable de cada componente de la plataforma tecnológica deberá realizar el monitoreo permanente sobre este.

27 PROTECCION CONTRA SOFTWARE MALICIOSO - *Ref: ISO/IEC 27001:2005 CL. A.10.4.*

a. Los sistemas operacionales y aplicaciones deberán actualizarse según lo definido en el procedimiento de Gestión de Vulnerabilidades Técnicas y Control de Cambios.

b. Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y seguridad de la información deberán estar protegidos mediante herramientas y software de seguridad que prevengan el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos dados por código móvil y malicioso.

c. Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin autorización de la Unidad de Informatica y deberán ser actualizados permanentemente.

d. No está permitido descargar software o archivos de fuentes externas a los recursos institucionales a través de Internet u otra red pública.

e. No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier equipo o red institucional.

f. Todos los medios de almacenamiento que se conecten a equipos del Hospital Militar Central deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la seguridad de la información corporativa.

g. El código móvil sólo podrá ser utilizado si proviene de sitios de confianza y es autorizado por el Oficial de Seguridad de la Información(o quien hagan sus veces).

h. El Hospital Militar Central será responsable de que sus usuarios se mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas Web, el intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza.

i. Los sistemas, equipos e información institucionales deberán ser revisados periódicamente para verificar que no haya presencia de código malicioso.

28 COPIAS DE RESPALDO - *Ref: ISO/IEC 27001:2005 CL. A.10.5.1.*

a. Se debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por la Unidad de Informática y las dependencias responsables de la misma, contenida en la plataforma tecnológica del Hospital Militar Central, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad, según lo definido en el Procedimiento Gestión de Copias de Respaldo y recuperación.

b. Los medios de las copias de respaldo se almacenarán localmente y en un sitio de custodia externa, garantizando en ambos casos la presencia de mecanismos de protección ambiental como detección de humo, fuego, humedad, así como mecanismos de control de acceso físico.

c. Se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

d. Para garantizar que la información de los funcionarios, contratistas y demás terceros autorizados sea respaldada, es responsabilidad de cada uno mantener copia de la información que se maneje.

e. La Unidad de Informática, establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma.

f. Se debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

29 GESTION DE MEDIOS REMOVIBLES - *Ref: ISO/IEC 27001:2005 CL. A.10.7.1.*

a. Se encuentra restringida la conexión no autorizada a la infraestructura tecnológica del Hospital Militar Central, de cualquier elemento de almacenamiento como dispositivos personales USB, discos duros externos, CDs, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, módems, entre otros dispositivos no institucionales.

b. Los medios de almacenamiento removibles como cintas, discos duros removibles, CDs, DVDs, medios impresos y dispositivos USB, entre otros, que contengan información institucional, deben ser controlados y físicamente protegidos.

c. El Hospital Militar Central definirá los medios removibles de almacenamiento que podrán ser utilizados por las personas autorizadas por el oficial de seguridad de la información (o quien haga sus veces), en los sistemas de información y en la plataforma tecnológica si es requerido para el cumplimiento de sus funciones.

d. Cada medio removible de almacenamiento deberá estar identificado de acuerdo con el tipo de información que almacene, dando cumplimiento a los lineamientos establecidos en el Procedimiento de Inventario y Clasificación de Activos de Información. Si un medio removible llegase a contener información con distintos

niveles de clasificación, será clasificado con la categoría que posea el mayor nivel de clasificación.

e. Para los procesos de baja, reutilización o garantías de los dispositivos que contengan medios de almacenamiento, se debe cumplir según sea el caso con la destrucción física del mismo o borrado seguro. La destrucción segura se documenta mediante acta, registro fílmico y fotográfico.

f. El tránsito o préstamo de medios removibles deberá ser autorizado por el responsable de dicho activo.

30 COMPUTACION MOVIL - *Ref: ISO/IEC 27001:2005 CL. A.11.7.*

a. Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, se deben implementar controles de acceso, técnicas criptográficas para cifrar la información crítica almacenada en estos, mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la seguridad de la información.

b. La conexión de los dispositivos móviles a la infraestructura tecnológica institucional deberá ser autorizada por el Oficial de Seguridad de la Información y la Unidad de Informatica, previa verificación de que cuenten con las condiciones de seguridad, estableciendo mecanismos de control necesarios para proteger la infraestructura.

31 GESTION DE REGISTROS - *Ref: ISO/IEC 27001:2005 CL. A.10.10.*

a. Tanto los sistemas de información que manejan información crítica, como los dispositivos de procesamiento, de red y de seguridad informática deberán generar registros de eventos que serán verificados periódicamente con el fin de detectar actividades no autorizadas sobre la información, siguiendo el procedimiento Monitoreo y Revisión de "*Logs*".

b. El tiempo de retención de los "*logs*" estará dado por las condiciones específicas de cada sistema de información, recurso informático o dispositivo de red y por las leyes, normativas o regulaciones que rigen al Sector Defensa.

c. El lugar de retención de los registros estará definido por el nivel de clasificación de información que posean dichos registros.

d. Todo aquel evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la integridad, disponibilidad o confidencialidad de

la infraestructura tecnológica deberá ser reportado al Oficial de Seguridad de la Información mediante el procedimiento de Gestión de Incidentes de seguridad.

32 CONTROL DE ACCESO - *Ref: ISO/IEC 27001:2005 CL. A.11.*

a. Los sistemas de información y dispositivos de procesamiento, seguridad informática y comunicaciones contarán con mecanismos de identificación de usuarios y procedimientos para el control de acceso a los mismos.

b. El acceso a los activos de información institucionales estará permitido únicamente a los usuarios autorizados por el responsable de cada activo, según el procedimiento Gestión de Usuarios y Contraseñas.

c. Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de procesamiento o seguridad informática del Sector Defensa deberá estar autorizado por la Unidad de Informatica y por el correspondiente Oficial de Seguridad de la Información.

d. Todas las conexiones remotas deberán ser autenticadas y seguras antes de conceder el acceso y el tráfico de datos deberá estar cifrado.

e. La creación, modificación y baja de usuarios en la infraestructura de procesamiento de información, comunicaciones y seguridad informática deberá seguir el procedimiento Gestión de Usuarios y Contraseñas.

f. Todo identificador de usuario establecido para un tercero o contratista, debe tener una fecha de vencimiento especificada, la cual en ningún caso debe superar la fecha de sus obligaciones contractuales.

g. La asignación de privilegios en las aplicaciones para los diferentes identificadores de usuario estarán determinados por el procedimiento Gestión de Usuarios y Contraseñas y deben revisarse a intervalos regulares y modificar o reasignar estos cuando se presenten cambios en el perfil del usuario, ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.

h. Los equipos de contratistas y demás terceros que requieran acceder a la redes de datos del Hospital Militar Central deben cumplir un procedimiento de sanitización informática antes de concedérseles dicho acceso.

i. Los equipos de contratistas y demás terceros que hayan sido autorizados para acceder de forma permanente a una o varias de las redes de datos institucionales,

sólo podrán hacerlo una vez se haya cumplido con el procedimiento inicial de formateo de discos duros y/o medios de almacenamiento, y posteriormente deben permanecer dentro de las respectivas instalaciones hasta la finalización del contrato o las labores para las cuales estaba definido.

c. Los accesos a la red inalámbrica deberán ser autorizados por la Unidad de Informática y por el correspondiente Oficial de Seguridad de la información), previa verificación de que cuenten con las condiciones de seguridad, estableciendo mecanismos de control necesarios para proteger la infraestructura.

33 ADMINISTRACION DE CONTRASEÑAS - *Ref: ISO/IEC 27001:2005 CL. A.11.2.*

a. La administración así como la entrega de las contraseñas a los usuarios deberá seguir el procedimiento Gestión de Usuarios y contraseñas.

b. Los usuarios deberán seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:

1. Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.

2. Las contraseñas no deberán ser reveladas.

3. Las contraseñas no se deberán escribir en ningún medio, excepto para los casos de administradores, cuando son entregadas en custodia de acuerdo con el procedimiento Gestión de Usuarios y Contraseñas.

4. Es deber de cualquier funcionario, contratista y/o tercero reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.

5. Las características de las contraseñas empleadas en la infraestructura tecnológica deberán cumplir los requerimientos definidos en el procedimiento de Gestión de Usuarios y Contraseñas.

34 BLOQUEO DE SESION, ESCRITORIO Y PANTALLA LIMPIA - *Ref: ISO/IEC 27001:2005 CL. A.11.3.2. y CL. A.11.3.3.*

a. En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar los medios que contengan información crítica protegida bajo llave.

b. Los usuarios deberán bloquear su estación cada vez que se retiren de su puesto de trabajo y sólo se podrá desbloquear con la contraseña del usuario.

c. Todas las estaciones de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido por la Unidad de Informatica, el cual se activará automáticamente después del tiempo de inactividad definido en el procedimiento de Gestión de Usuarios y Contraseñas, y se podrá desbloquear únicamente con la contraseña del usuario.

d. Los usuarios deberán retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.

e. No se deberá reutilizar papel que contenga información sensible.

f. Los usuarios no deberán almacenar en el escritorio de sus estaciones de trabajo documentos, accesos directos a los mismos o a sistemas de información sensibles.

g. Los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados, por lo tanto debe estar presente en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos.

35 ANALISIS Y ESPECIFICACIONES DE REQUERIMIENTOS DE SEGURIDAD - *Ref: ISO/IEC 27001:2005 CL. A.12.1.1.*

a. Todas las solicitudes para compra, actualización y/o desarrollo de software deberán estar aprobadas por la Unidad de Informatica.

36 CONTROL DE VERSIONES - *Ref: ISO/IEC 27001:2005 CL. A.12.4.3 y CL. A.12.5.1.*

a. Antes de la puesta en producción de una aplicación nueva, o de la modificación de las plataformas existentes, se debe asignar un número de edición o versión a la misma. Así, el número de versión se irá incrementando en cada cambio que se genere sobre la misma aplicación, de acuerdo con el procedimiento Control de Versiones.

b. El método de enumeración de las versiones deberá distinguir entre versiones en producción, en etapa de desarrollo, en etapa de pruebas o versión archivada.

c. Todas las versiones deben ser almacenadas en bibliotecas, repositorios o directorios y deben contar con controles de acceso lógicos donde sólo se permita el acceso al personal autorizado.

d. Periódicamente, las versiones que se encuentran en los ambientes de producción deben ser verificadas contra los repositorios y la documentación de los controles de cambio con el fin de determinar si los dos son congruentes. Si llegase a presentarse incongruencia en la revisión realizada, esto será identificado como un incidente de seguridad y se atenderá de acuerdo con el procedimiento de Gestión de Incidentes de seguridad.

37 CONTROLES CRIPTOGRAFICOS - *Ref: ISO/IEC 27001:2005 CL. A.12.3.*

a. La Unidad de Informática, debe identificar, definir e implementar mecanismos y controles criptográficos para garantizar el cumplimiento de los objetivos de seguridad definidos, en términos de protección de la confidencialidad de la información en medio electrónico, de acuerdo con los lineamientos definidos en el procedimiento de Inventario y Clasificación de Activos de Información, tanto cuando se encuentra almacenada como cuando es transmitida o procesada, teniendo en cuenta la clasificación y sensibilidad de la información.

b. No se permite el uso de herramientas o mecanismos de cifrado de información diferentes a las autorizadas por la Unidad de Informática, los cuales deben estar documentados en una lista de software autorizado que sea divulgada a todos los funcionarios, contratistas y demás terceros autorizados.

38 GESTION DE VULNERABILIDADES TECNICAS - *Ref: ISO/IEC 27001:2005 CL. A.12.6.*

a. La Unidad de Informática se encargará de identificar las vulnerabilidades técnicas de las diferentes plataformas tecnológicas y para esto definirá las herramientas y/o servicios necesarios.

b. La Unidad de informática será responsable de proponer y ejecutar un programa de evaluación y gestión de vulnerabilidades que debe ser utilizado para la plataforma tecnológica de la dependencia o entidad.

c. No se permite a los usuarios de los activos informáticos, sin la autorización expresa del Oficial de Seguridad de la Información o quien haga sus veces, realizar o participar por iniciativa propia o de terceros, en pruebas de acceso o ataques activos o pasivos a los activos informáticos del Hospital Militar Central, o a la utilización de los mismos para efectuar pruebas de vulnerabilidad o ataques a otros equipos o sistemas externos.

d. Los administradores de las plataformas y sistemas de información serán responsables de mantener protegida la infraestructura a su cargo de los riesgos derivados de las vulnerabilidades técnicas identificadas.

e. El Área de Seguridad de la Información (o las que hagan sus veces), realizará el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas.

f. Periódicamente, la correspondiente Área de Seguridad de la Información realizará una verificación de alertas de seguridad emitidas por organizaciones y foros de seguridad de la información de orden nacional y/o internacional, con el fin de verificar la información más reciente que se encuentre disponible respecto a vulnerabilidades y eventos de seguridad que se hayan presentado o que sean susceptibles de ocurrencia.

g. En caso de encontrar información crítica respecto a amenazas o vulnerabilidades que puedan afectar las plataformas tecnológicas, la correspondiente Área de Seguridad de la Información deberá generar una comunicación oficial a la Unidad de Informática con el fin de que se tomen inmediatamente las acciones preventivas necesarias para evitar algún impacto a la plataforma tecnológica.

h. La Unidad de Informática realizará las revisiones de las alertas de seguridad informada por el área de seguridad de la Información y dado el caso en que las alertas sean válidas en el entorno de operación de las plataformas tecnológicas asociadas, se deberá definir un plan de acción para mitigar el impacto de las mismas en los ambientes de producción y desarrollo de la infraestructura tecnológica.

39 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION - *Ref: ISO/IEC 27001:2005 CL. A. A.13.1. y CL. A.13.2.*

a. Los funcionarios, contratistas y terceras partes del Hospital Militar Central deberá informar cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.

b. Para gestionar los incidentes de seguridad de la información deberá existir como mínimo un funcionario con conocimientos en el manejo de incidentes en las Áreas de Seguridad de la información.

c. Los incidentes reportados de mayor complejidad o que no puedan ser solucionados, deberán ser escalados a los CSIRT del Sector Defensa.

d. Para los casos en que los incidentes reportados requieran judicialización se deberá coordinar con los organismos que cuentan con función de policía judicial.

e. Se debe llevar un registro detallado de los incidentes de seguridad de la información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo y, de ser posible, la valoración de los daños.

f. El Área de Seguridad de la Información debe propender por la adquisición de herramientas que faciliten el proceso de gestión de incidentes de seguridad de la información.

g. El Hospital Militar Central deberá establecer los mecanismos de control necesarios para recolectar y preservar la evidencia de las investigaciones que se realicen durante el análisis de un incidente de seguridad de la información.

40 SEGURIDAD DE LA INFORMACION EN LA CONTINUIDAD DEL NEGOCIO - *Ref: ISO/IEC 27001:2005 CL. A.14.1.*

a. La seguridad de la información es una prioridad y se incluye como parte de la gestión general de la continuidad del negocio y del compromiso de la Alta Dirección.

b. El Hospital Militar Central deberá contar con un Plan de Continuidad del Negocio que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales.

c. Para el Hospital Militar Central su activo más importante es el recurso humano y por lo tanto será su prioridad y objetivo principal establecer las estrategias para mantenerlo.

d. Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan, estarán incorporados y definidos en el Plan de Continuidad de Negocio.

e. Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados e informar cualquier cambio al responsable de la gestión del Plan de Continuidad de Negocio.

41 DERECHOS DE PROPIEDAD INTELECTUAL - *Ref: ISO/IEC 27001:2005 CL. A.15.1.2.*

a. El Hospital Militar Central cumplirá con la reglamentación de propiedad intelectual, para lo cual implementarán los controles necesarios que garanticen el cumplimiento de dicha reglamentación.

b. No se permitirá el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.

c. Se permitirá el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de los mismos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.

d. Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

e. El desarrollo de software a la medida adquirido a terceras partes o realizados por funcionarios del Hospital Militar Central, serán de uso exclusivo de dicha entidad y la propiedad intelectual será de quien lo desarrolle.

42 SANCIONES PREVISTAS POR INCUMPLIMIENTO - *Ref: ISO/IEC 27001:2005 CL. A.15.1*

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente política de seguridad, conforme a lo dispuesto por las normas estatutarias escalonarías y convencionales que rigen al personal del Hospital Militar Central y en caso de

corresponder, se realizarán las acciones correspondientes ante el o los organismos pertinentes.

Las sanciones solo pueden imponerse mediante un acto administrativo que así lo disponga, cumpliendo las formalidades impuestas por los preceptos constitucionales, la ley de procedimientos administrativos y demás normativas específicas aplicables.

Además de las sanciones disciplinarias o administrativas la persona que no da debido cumplimiento a sus obligaciones, puede incurrir también en responsabilidad civil o patrimonial, cuando ocasiona un daño que debe ser indemnizado y/o en responsabilidad penal cuando su conducta constituye un comportamiento considerado delito por el código penal y leyes especiales.

FEB

Notifíquese Y Cúmplase;

Mayor General (RA) Luis Eduardo Perez Arango
Director General Entidad Descentralizada Hospital Militar Central

VoBo Unidad de Informatica
Mayor Ariadna Ramirez Ospina
Jefe Unidad de informatica

VoBo Oficina Asesora Jurídica
Denys Adíela Ortiz Alvarado
Jefe Oficina Asesora Jurídica

Revisó:
Ing. Fabio Alvarado
Profesional de Defensa
Unidad de Informatica

Revisó:
Abogada Carolina correa
Contratista
Oficina Asesora Jurídica