



**HOSPITAL
ROBERTO QUINTERO VILLA**
E.S.E. MONTENEGRO
La Salud... Nuestro compromiso
NIT. 890.000.400-2

**PLAN DE TRATAMIENTO DE
RIESGOS DE SEGURIDAD Y
PRIVACIDAD DE LA
INFORMACION**

Código: 51-014

Versión: 001

Fecha: 30 01 2019

Página 1 de 26

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

MYRIAM BEJARANO PULIDO

Gerente

VIGILADO Supersalud
Línea de Atención al Usuario: 665.00.870 – Bogotá, D.C.
Línea Gratuita Nacional: 01.800.00.10388

VIGENCIA

2019



Certificado No. SC-5858-1





CONTENIDO

INTRODUCCIÓN	3
1. JUSTIFICACIÓN.....	4
2. GLOSARIO	5
3. OBJETIVOS.....	18
3.1 OBJETIVO GENERAL	18
3.2 OBJETIVOS ESPECÍFICOS.....	18
4. ETAPAS PARA LA GESTIÓN DEL RIESGO.....	18
4.1 COMPONENTES:	19
4.2 ESTRUCTURA PARA LA GESTIÓN DEL RIESGO:	20
4.3 IDENTIFICACIÓN DEL RIESGO	21
4.4 PLAN DE TRATAMIENTO DE RIESGOS	23
5. INDICADORES - GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL.	24
6. INFORMACIÓN, COMUNICACIÓN Y REPORTE:	25
BIBLIOGRAFIA	26



HOSPITAL
ROBERTO QUINTERO VILLA
E.S.E. MONTENEGRO
La Salud... Nuestro compromiso
NIT. 890.000.400-2

**PLAN DE TRATAMIENTO DE
RIESGOS DE SEGURIDAD Y
PRIVACIDAD DE LA
INFORMACION**

Código: 51-014

Versión: 001

Fecha: 30 01 2019

Página 3 de 26

INTRODUCCIÓN

La información que hace parte de una Entidad Pública es crucial para su correcto desempeño dentro de la política pública y su relación con el ciudadano, sin importar qué tipo de información se trate en la Entidad, ésta será parte primordial en el cumplimiento de sus Objetivos, es por ello que resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de una Entidad o de un Estado.

La gestión de riesgos es un aspecto decisivo dentro el Plan de Seguridad y Privacidad de la información y se desarrolla siguiendo los lineamientos establecidos por el Departamento Administrativo de la Función Pública en su “Guía para la administración del riesgo de gestión, de corrupción y de seguridad digital y diseño de controles en las entidades pública.

La ESE acoge la gestión de riesgos como un proceso sistemático de identificación, análisis, evaluación, valoración, y tratamiento de los riesgos; aplicando los controles necesarios para evitar, reducir, compartir, transferir o asumir el riesgo con medidas preventivas o correctivas que deberá generar como resultado minimizar pérdidas, maximizar rendimientos y cuidar la seguridad del paciente.


VIGILADO Supersalud
Línea de Atención al Usuario: 665.0870 – Bogotá, D.C.
Línea Gratuita Nacional: 01 800 09 10388



Certificado No. SC-5858-1





1. JUSTIFICACIÓN

El avance tecnológico y el uso masivo de las tecnologías de la información y las comunicaciones (TIC) han permitido optimizar las actividades ejecutadas por las entidades colombianas ya sean de carácter público, privado o de cualquier índole. Este avance ha incrementado el uso de las TIC, particularmente en la prestación de servicios esenciales a la nación.

Así mismo, los cambios provocados por la evolución continua de la tecnología, y en general de las redes informáticas, han inclinado a algunas entidades y ciudadanos a utilizarlas como medios para incrementar su productividad, para ser más competitivos en los negocios, para satisfacer necesidades propias y para generar valor. Por otra parte, en otros escenarios se ha incrementado el uso de la tecnología con fines delictivos o para generar amenazas informáticas; este propósito busca afectar otras infraestructuras tecnológicas, sistemas de información financieros, personas e, incluso, llegar a impactar la economía de toda una nación. Es por esta razón, que los estados han incrementado su preocupación por los riesgos a los que puedan estar expuestas las instituciones (entidades, organizaciones, empresas y la misma ciudadanía) y han decidido incluir en sus planes estratégicos modelos de ciberseguridad y ciberdefensa encaminados básicamente a fortalecer la seguridad de su nación y por ende, de todos los que la componen.

Es por ello que siguiendo los lineamientos técnicos del Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC, se ha elaborado un Plan de Seguridad y Privacidad de la información, y un plan de tratamiento de riesgos de seguridad y privacidad de la información de conformidad con las prácticas nacionales e internacionales para la gestión de riesgos y tiene como fin contribuir al aprovechamiento de un entorno digital seguro, permitiéndole a la entidad gestionar los riesgos que afectan sus procesos misionales donde se involucran tecnologías de operación que son críticas para el sector salud.



2. GLOSARIO

Acceso a la información pública

Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Actitud hacia el riesgo

Enfoque de la organización para evaluar y eventualmente buscar, retener, tomar o alejarse del riesgo. (NTC ISO 31000:2011).

Activo

Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854:2016, pág.56).

Activo cibernético

En relación con la privacidad de la información, se refiere al activo que contiene información que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Amenaza

Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO 2700:2016).

Amenaza cibernética

Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854).



Análisis del riesgo

Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011).

Apetito de riesgo

Es el máximo nivel de riesgo que los accionistas están dispuestos a aceptar. (Componente COSO ERM II)

Ataque cibernético

Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia).

CCOC

Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia CoLCERT.

CERT

Computer Emergency Response Team (Equipo de respuesta a emergencias cibernéticas). (Universidad Carnegie-Mellón).

Cibercrimen (Delito cibernético)

Conjunto de actividades ilegales asociadas con el uso de las tecnologías de la información y las comunicaciones, como fin o como medio. (CONPES 3854, pág. 87).

Ciberdefensa

Es el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. (CONPES 3854, pág. 88).



Ciberseguridad

Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio. (CONPES 3854, pág. 87).

Ciberterrorismo

Es el uso del ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o Estado trayendo como consecuencia una violación a la voluntad de las personas. (CONPES 3854, pág. 88).

Ciberdelincuencia

Acciones ilícitas que son cometidas mediante la utilización de un bien o servicio informático. (Ministerio de Defensa de Colombia).

Ciberdelito/Delito cibernético

Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia).

Ciberespacio

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Cibernética Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas. (Diccionario de la lengua española).



Cibernético

Adjetivo masculino y femenino para denominar todo cuanto tiene relación con la cibernética: órgano cibernético, proceso cibernético o que está especializado en cibernética, así como también a la persona que se dedica a ella. (Diccionario de la lengua española).

Convergencia

Evolución coordinada de redes que antes eran independientes hacia una uniformidad que permita el soporte común de servicios y aplicaciones. (Rec. UIT-T Q.1761, 3.1).

CSIRT

Por su sigla en inglés: *Computer Security Incident Response Team* (Equipo de respuesta a incidentes de seguridad cibernética). ([http:// www.first.org](http://www.first.org)).

Comunicación y consulta

Procesos continuos y reiterativos que una organización lleva a cabo para suministrar, compartir u obtener información e involucrarse en un diálogo con las partes involucradas con respecto a la gestión del riesgo. (NTC ISO 31000:2011).

Consulta

La consulta es un proceso de doble vía de la comunicación informada entre una organización y sus partes involucradas, acerca de algún tema, antes de tomar una decisión o determinar una dirección para dicho tema. La consulta es: un proceso que tiene impacto en la decisión a través de la influencia más que del poder; y: una entrada para la toma de decisiones, no para la toma conjunta de decisiones. (NTC ISO 31000 definición 2.12.).

Compartir el riesgo

Compartir con otra de las partes el peso de la pérdida o el beneficio de la ganancia proveniente de un riesgo particular. (NTC ISO 31000:2011).

Conocimiento, capacidades y empoderamiento

Las múltiples partes interesadas deben entender los riesgos de seguridad digital. Deben ser conscientes de que el riesgo de seguridad digital puede afectar el logro



de sus objetivos económicos y sociales, y el de otros. Deben estar educados al respecto, poseer las habilidades necesarias para entender el riesgo, administrarlo y evaluar su impacto. (CONPES 3854, pág. 25).

Consecuencia

Resultado o impacto de un evento que afecta a los objetivos. (NTC ISO 31000:2011).

Contexto externo

Ambiente externo en el cual la organización busca alcanzar sus objetivos. (NTC ISO 31000:2011).

Contexto interno

Ambiente interno en el cual la organización busca alcanzar sus objetivos. (NTC ISO 31000:2011).

Control

Medida que modifica al riesgo. (NTC ISO 31000:2011), medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Cooperación

Las múltiples partes interesadas deben cooperar, incluso más allá de sus fronteras, a nivel regional e internacional.

Criterios del riesgo

Términos de referencia frente a los cuales se evalúa la importancia de un riesgo. (NTC ISO 31000:2011).

Derechos humanos y valores fundamentales

Las múltiples partes interesadas deben gestionar los riesgos de seguridad digital de manera transparente y compatible con los derechos humanos y los valores fundamentales. La implementación de la gestión de riesgos de seguridad digital debe ser compatible con la libertad de expresión, el libre flujo de la información, la



confidencialidad de la información, la protección de la privacidad y los datos personales. Las organizaciones deben tener una política general de transparencia acerca de sus prácticas y procedimientos para la gestión de riesgos de seguridad digital.

Entorno digital

Ambiente, tanto físico como virtual, sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854, pág. 87).

Entorno digital abierto

En el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).

Establecimiento del contexto

Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo y establecimiento del alcance y los criterios del riesgo para la política para la gestión del riesgo. (NTC ISO 31000:2011).

Evaluación del control

Revisión sistemática de los procesos para garantizar que los controles son adecuados y eficaces. (NTC ISO 31000:2011).

Evaluación del riesgo

Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables. (NTC ISO 31000:2011).



Evento de seguridad de la información

Ocurrencia que indica una posible brecha de seguridad de la información o falla de los controles. (ISO/IEC 27035:2016).

Evitar el riesgo

Decisión de no involucrarse o de retirarse de una situación de riesgo. (NTC ISO 31000:2011).

Evento

Presencia o cambio de un conjunto particular de circunstancias. (NTC ISO 31000:2011).

Fuente de riesgo

Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo. (NTC ISO 31000:2011).

Frecuencia

Medición del número de ocurrencias por unidad de tiempo. (NTC ISO 31000:2011).

Gestión del riesgo

Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. (NTC ISO 31000:2011).

Gestión de riesgos de seguridad digital

Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego. (CONPES 3854, pág. 24).



ICC

Es la denominación de lo que el CCOC ha definido como infraestructuras críticas cibernéticas en el ámbito colombiano.

Identificación del riesgo

Proceso para encontrar, reconocer y describir el riesgo. (NTC ISO 31000:2011).

Incidente digital

Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).

Incidente de seguridad de la información

Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones. (ISO/IEC 27035:2016).

Infraestructura crítica cibernética nacional

Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (CONPES 3854, pág. 29).

Inventario de activos

Sigla en inglés: *Assets inventory*. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos (ISO 27000.ES).

ISO

Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización, cuyo objetivo es establecer, promocionar y gestionar estándares. (<http://www.iso.org>).



Marco de referencia para la gestión del riesgo

Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo, a través de toda la organización. (NTC ISO 31000:2011).

Monitoreo

Verificación, supervisión, observación crítica o determinación continua del Estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado. (NTC ISO 31000:2011).

Múltiples partes interesadas

El Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la fuerza pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades. (CONPES 3854, pág. 29).

Nivel de riesgo

Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad. (NTC ISO 31000:2011).

Organización

Grupo de personas e instalaciones con distribución de responsabilidades, autoridades y relaciones. (NTC ISO 31000:2011).

Parte involucrada

Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada, por una decisión o una actividad. (NTC ISO 31000:2011).

Peligro

Una fuente de daño potencial. (NTC ISO 31000:2011).



Pérdida

Cualquier consecuencia negativa o efecto adverso, financiero u otro. (NTC ISO 31000:2011).

Perfil del riesgo

Descripción de cualquier conjunto de riesgos. (NTC ISO 31000:2011).

Política

Intenciones y dirección de una organización como las expresa formalmente su alta dirección. (ISO/IEC 27000:2016).

Política para la gestión del riesgo

Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. (NTC ISO 31000:2011).

Posibilidad

Se utiliza como descripción general de la probabilidad o la frecuencia. (NTC ISO 31000:2011).

Plan para la gestión del riesgo

Esquema dentro del marco de referencia para la gestión del riesgo que especifica el enfoque, los componentes y los recursos de la gestión que se van a aplicar a la gestión del riesgo. (NTC ISO 31000:2011).

Probabilidad

Oportunidad de que algo suceda. (NTC ISO 31000:2011).

Proceso para la gestión del riesgo

Aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo. (NTC ISO 31000:2011).



Propietario del riesgo

Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo. (ISO GUIA 73:2009).

Responsabilidad

Las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás. Deben también reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales. (CONPES 3854, pág. 25).

Revisión

Acción que se emprende para determinar la idoneidad, conveniencia y eficacia de la materia en cuestión para lograr los objetivos establecidos. (NTC ISO 31000:2011).

Reducción del riesgo

Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo. (NTC ISO 31000:2011).

Resiliencia

Es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (CONPES 3854, pág. 87).

Retención del riesgo

Aceptación del peso de la pérdida o del beneficio de la ganancia proveniente de un riesgo particular. (NTC ISO 31000:2011).

Riesgo

Efecto de la incertidumbre sobre los objetivos. (NTC ISO 31000:2011).



Riesgo inherente

Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. (NTC ISO 31000:2011).

Riesgo residual

Remanente después del tratamiento del riesgo. (NTC ISO 31000:2011).

Seguridad de la información

Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. (ISO/IEC 27001:2016).

Seguridad digital

Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854, pág. 29).

Servicios esenciales

Los necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las administraciones públicas (Tomado del documento ICC del CCOC).

SGC

Sistema de gestión de calidad.

SGSI

Sistema de gestión de seguridad de la información.

Sistema para la gestión del riesgo

Conjunto de elementos del sistema de gestión de una organización involucrados en la gestión del riesgo. (NTC ISO 31000:2011).



Telecomunicaciones

Toda transmisión y recepción de signos, señales, escritos, imágenes y sonidos, datos o información de cualquier naturaleza por hilo, radiofrecuencia, medios ópticos u otros sistemas electromagnéticos. (Resolución MinTIC 202 de 2010).

TI

Tecnologías de la información.

TO

Tecnología de operación

TIC (Tecnologías de la información y las comunicaciones)

Conjunto de recursos, herramientas, equipos, programas informáticos aplicaciones, redes y medios que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes. (Ley 1341/2009 TIC).

Tratamiento del riesgo

Proceso para modificar el riesgo. (ISO/IEC Guía 73:2009).

Valoración del riesgo

Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo. (ISO GUÍA 73:2009).

Vulnerabilidad

Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87).

 HOSPITAL ROBERTO QUINTERO VILLA E.S.E. MONTENEGRO <i>La Salud... Nuestro compromiso</i> <small>NIT. 890.000.400-2</small>	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: 51-014
		Versión: 001
		Fecha: 30 01 2019
		Página 18 de 26

3. OBJETIVOS

3.1 OBJETIVO GENERAL

gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP

3.2 OBJETIVOS ESPECÍFICOS

- Establecer la metodología para la gestión de riesgos de seguridad digital en la entidad.
- Fomentar un modelo de comunicación y de colaboración en la gestión de los riesgos digitales, entre las múltiples partes interesadas;
- Servir de base para facilitar a todo nivel la toma de decisiones sobre aspectos relacionados con la seguridad digital.

4. ETAPAS PARA LA GESTIÓN DEL RIESGO

- a) Compromiso de las alta y media dirección: Tener el verdadero compromiso de los directivos garantizan en gran medida el éxito de cualquier proceso emprendido, puesto que se necesita su aprobación y concurso en el momento de cualquier toma de decisiones.
- b) Conformación de un equipo interdisciplinario, la idea de una integralidad en el tratamiento de los riesgos para poder tener una visión completa de la Entidad y en la cual se pueda tener el aporte de diferentes áreas analizando un mismo proceso, es esencial y ayuda a encaminar correctamente el Plan de Seguridad



y Privacidad de la Información, es por esta razón que se deben incluir los riesgos de seguridad en el momento que se hace el análisis para el MECI, o para el Sistema de Gestión de Calidad.

- c) Capacitación en la metodología: El equipo interdisciplinario debe capacitarse para poder analizar los riesgos de seguridad.

4.1 COMPONENTES:

- ✓ **Planificación de la GRSD:** Consiste en la definición de contextos, variables para posterior análisis y evaluación de riesgos y en general todos los aspectos que se desarrollarán en los demás componentes.
- ✓ **Ejecución de la GRSD:** Consiste en el desarrollo de las actividades para el análisis y evaluación de los riesgos de seguridad digital, se identifican aspectos inherentes y residuales de los mismos, así como la definición del tratamiento de los riesgos en el marco de la seguridad de la información y particularmente en las ICC.
- ✓ **Monitoreo y Revisión de la GRSD:** Consiste en la permanente evaluación que permita asegurar que dicha gestión se está llevando a cabo bajo los aspectos y lineamientos definidos por la entidad para sus riesgos de seguridad digital. Se desprenden aspectos de reporte y aseguramiento del seguimiento de todos los planes de tratamiento que se derivan de su aplicación.
- ✓ **Mejora de la GRSD:** Componente que tiene una orientación para establecer los mecanismos que permitan alcanzar un mayor grado de madurez de la GRSD en cualquier entidad. El mejoramiento continuo se estará dando de forma progresiva en la medida que se cumplan con los objetivos de la GRSD así como la definición y aplicación modelos de evaluación de riesgos de seguridad digital con una orientación menos subjetiva y basada en modelos matemáticos que brinden mayor exactitud en la medición de las variables de impacto de los riesgos de seguridad digital sobre los activos de información y las ICC identificadas.



4.2 ESTRUCTURA PARA LA GESTIÓN DEL RIESGO:

La metodología a utilizar para la gestión del riesgo es la definida por el DAFP en su “Guía para la administración del riesgo de gestión, de corrupción y de seguridad digital y diseño de controles en las entidades públicas”, para lo cual se debe:

- Incluir los aspectos relevantes sobre los factores de riesgo estratégicos para la entidad, a partir de los cuales todos los procesos podrán iniciar con los análisis para el establecimiento del contexto.
- Incluir la periodicidad para el monitoreo y revisión de los riesgos. Incluir los niveles de riesgo aceptado para la entidad y su forma de manejo.
- Incluir la tabla de impactos institucional y Niveles para Calificar el Impacto o Consecuencias
- Otros aspectos que la entidad considere necesarios deberán ser incluidos, con el fin de generar orientaciones claras y precisas para todos los funcionarios, de modo tal que la gestión del riesgo sea efectiva y esté articulada con la estrategia de la entidad.





4.3 IDENTIFICACIÓN DEL RIESGO

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de **seguridad digital** son activos elementos tales como (Aplicaciones de la organización, Servicios Web, Redes, Información física o digital, **TI, TO**) que utiliza la organización para funcionar en el **entorno digital**.

Activos de información

Es importante resaltar que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación; es decir que en los criterios de Confidencialidad, Integridad y Disponibilidad tengan la siguiente calificación:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PÚBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 1. Criterios de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Tabla 2. Niveles de Clasificación

IDENTIFICACION DEL RIESGO

Ejemplo:

ACTIVO	RIESGO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS Vulnerabilidades	CONSECUENCIAS
Base de datos Cnt y workmanager	<i>Pérdida de la integridad</i>	La falta de políticas de seguridad, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada causando la pérdida de la integridad de la base de datos de Cnt y workmanager.	Modificación no autorizada	Seguridad Digital	<p>Falta de políticas de seguridad.</p> <p>Ausencia de políticas de control de acceso.</p> <p>Contraseñas sin protección</p> <p>Autenticación débil</p>	<i>Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo. (Legales, económicas, sociales, reputacionales, confianza en el ciudadano).</i>

4.4 PLAN DE TRATAMIENTO DE RIESGOS

Nr o	Activo	Riesgo	Tipo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo Residual	Opción Tratamiento	Actividad Control	de Soporte	Responsable	Tiempo	Indicador
1	Base de Datos de Nómina	Pérdida de la integridad	Seguridad Digital	Modificación no autorizada	Ausencia de políticas de control de acceso.	Probable	M a	Extremo	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	Ver Siguiete Página
					Reducir				A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018		
					Reducir				A.9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Cuarto trimestre de 2018		
					Reducir				A.11.2.8 Equipos para bloqueo de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Cuarto Trimestre de 2018		



5. INDICADORES - GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL.

Igualmente, en el caso de los riesgos de seguridad digital, se deben generar indicadores, para medir la gestión realizada, en esencia la eficacia y la efectividad de los planes de tratamiento implementados.

La entidad deberá definir como mínimo 4 indicadores POR PROCESO de la siguiente manera:

1 indicador de Eficacia, que indique el cumplimiento de las actividades para la gestión del riesgo de seguridad digital en cada PROCESO de la entidad.

1 indicador de Efectividad, por cada criterio de seguridad digital (Confidencialidad, integridad y disponibilidad), según sea el caso.

Eficacia:

Porcentaje de controles implementados= ($\#$ controles implementados / $\#$ controles definidos) x 100

Efectividad:

$\#$ Riesgos materializados de Confidencialidad= ($\#$ de incidentes que afectaron la confidencialidad de algún activo del proceso)

Variación de Incidentes de Confidencialidad (Para entidades con mediciones anteriores)=

$((\#$ de Incidentes de Confidencialidad Periodo Actual - $\#$ de Incidentes de Confidencialidad Periodo Previo) / Incidentes de Confidencialidad Periodo Previo)*100%

 HOSPITAL ROBERTO QUINTERO VILLA E.S.E. MONTENEGRO <i>La Salud... Nuestro compromiso</i> <small>NIT. 890.000.400-2</small>	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Código: 51-014
		Versión: 001
		Fecha: 30 01 2019
		Página 25 de 26

6. INFORMACIÓN, COMUNICACIÓN Y REPORTE:

La comunicación de la Información y el reporte debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios. Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.

Por tanto se debe hacer especial énfasis en la difusión, socialización, capacitación y/o entrenamiento de todos y cada uno de los pasos que componen la metodología de la administración del riesgo, asegurando que permee a la totalidad de la organización pública.

Se debe conservar evidencia de la comunicación de la información y reporte de la administración del riesgo en todas sus etapas.

Adicionalmente, los riesgos de seguridad digital deberán ser reportados a MinTIC conforme lo indica la sección 3.3.3 del Anexo “Lineamientos para la gestión del riesgo de seguridad digital” de la presente guía.

JORGE IVAN MEJIA VILLANUEVA

Ingeniero de sistemas


VIGILADO Supersalud
 Línea de Atención al Usuario: 6650870 – Bogotá, D.C.
 Línea Gratuita Nacional: 01800 09 10388



Certificado No. SC-5858-1



 <p>HOSPITAL ROBERTO QUINTERO VILLA E.S.E. MONTENEGRO <i>La Salud... Nuestro compromiso</i> NIT. 890.000.400-2</p>	<p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</p>	Código: 51-014
		Versión: 001
		Fecha: 30 01 2019
		Página 26 de 26

BIBLIOGRAFÍA

Guía 7 gestión de riesgos. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea.

Guía 8 controles de seguridad y privacidad de la información. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea.

VIGILADO Supersalud
Línea de Atención al Usuario: 665.00870 – Bogotá, D.C.
Línea Gratuita Nacional: 01800.00.10388



Certificado No. SC-5858-1

