HOSPITAL DEPARTAMENTAL SAN VICENTE DE PAÚL E.S.E.
GARZÓN – HUILA

SEGURIDAD DIGITAL

EMPRESA SOCIAL DEL ESTADO
HOSPITAL DEPARTAMENTAL SAN VICENTE DE PAÚL
GARZON - HUILA

SEGURIDAD DIGITAL

PROCESO

GESTIÓN DE APOYO CORPORATIVO

JORGE HUMBERTO GONZALEZ BAHAMON
Gerente

ESPERANZA FIERRO VANEGAS
Subdirectora Administrativa

GARZON – HUILA

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

CUERPO DIRECTIVO EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN VICENTE DE PAUL.

JORGE HUMBERTO GONZALEZ BAHAMON
Gerente

YANETH GUTIERREZ MARTINEZ
Asesor de Control Interno

PABLO LEON PUENTES QUESADA
Subdirector Científico

ESPERANZA FIERRO VANEGAS
Subdirector Administrativo

LUIS FERNANDO CASTRO MAJE
Asesor Jurídico

MARIBEL CASTAÑO RODRIGEZ
Líder de Mejora Continua

JORGE HUMBERTO GONZALEZ BAHAMON
Coordinador Unidad Funcional Sistemas de Información
Autor(a).

GARZON HUILA

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

TABLA DE CONTENIDO

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

DEFINIR COMPETENCIAS PERSONAL SEGURIDAD DE LA INFORMACIÓN

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

INTRODUCCIÓN

La E.S.E Hospital Departamental San Vicente de Paul de Garzón, Es muy importante que Los profesionales participen en un grupo de diseño de sistemas informáticos. Administrar servicios informáticos o teleinformáticas.
Planificar, dirigir y controlar el relevamiento, diseño y ejecución de los proyectos, así como la implantación de sistemas de información en las organizaciones y entes de racionalidad económica.
Resolver problemas relacionados con el soporte físico, el soporte lógico, las comunicaciones y el procesamiento eficiente de uno de los recursos fundamentales de las instituciones.
Intervenir en equipos con enfoque interdisciplinario en proyectos de consultoría, auditoria informática, optimización de procesos de IT, etc., que requieran la integración profesional de los especialistas en sistemas con otras áreas del conocimiento.

1. PLANTEAMITENTO DEL PROBLEMA

Los principales propósitos que orientan la formación del Especialista en Sistemas de Información son:

- Para el Hospital Deben tener una amplia perspectiva del negocio y del mundo real y entender que los Sistemas de Información:

- Son uno de los grandes habilitadores del desempeño organizacional.
  Abarcan e integran todos los niveles organizacionales y a todas las funciones del negocio.
  Están incrementando su significancia estratégica.

2. MARCO TEORICO

La E.S.E Hospital Departamental San Vicente de Paul de Garzón, Deben tener unas fuertes competencias analíticas y críticas.
Deben demostrar fuertes principios éticos y tener buenas habilidades de comunicación interpersonal y de trabajo en equipo. Requieren:

Aplicar códigos de conducta profesional.
Colaborar con grupos interdepartamentales e interinstitucionales.

- Esfuerzo individual asertivo.
- Excelentes habilidades comunicativas para diseñar y gerencia su labor.
- Persistencia, curiosidad, creatividad, gestión del riesgo y tolerancia entre otras habilidades.
- Deben diseñar e implementar soluciones de TI que mejoren el desempeño organizacional.
- Deben poseer habilidades para entender y modelar los procesos y datos organizacionales, definir e implementar soluciones técnicas y de procesos, gerencia proyectos e integrar sistemas.
- Dominar técnicas para adquirir, convertir, transmitir y almacenar datos e información.
- Enfocarse en la aplicación de las tecnologías de información para ayudar a los individuos, grupos y organizaciones a alcanzar sus metas.

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

3. OBJETIVO

a. General

Para la E.S.E, es muy importante que el Profesional responda a dos preguntas: ¿Qué queremos? (cuales son mis intereses y qué motivaciones tenemos) y ¿qué podemos ofrecer? (es decir, nuestras aptitudes, actitudes, competencias, formación y experiencia). Igualmente lo podemos emplear para ponerlo en el currículum vitae y/o en la carta de presentación e incluso también nos sirve para la entrevista. Definir nuestro objetivo profesional nos permite conocer que puestos de trabajo vamos a buscar y que podemos ofrecer como posibles candidatos.

b. Específicos

Para ayudaros a realizar vuestro objetivo profesional podéis comenzar analizando vuestras experiencias en los siguientes apartados que os proponemos

- Tipo de empresa: (Pública, Privada, Mixta, Familiar…)
- Sector: (Educación, Sanidad, Hostelería…)
- Desarrollo de trabajo: (Funciones a desarrollar)
- Nivel (Auxiliar, Técnico, Gerente, Director…)
- Sueldo: (Siempre anual bruto)
- Horario: (Mañana, Tarde, Noche)
- Jornada: (Total, Parcial, Turnos…)
- Ámbito Geográfico: Nacional, Internacional…

Consideramos que, en el caso de tener escasa experiencia y/o no tener muy claro hacia dónde quiero enfocar mi experiencia profesional, es mejor dar énfasis al perfil personal/profesional, pero en caso contrario, dónde tenemos claro hacia dónde quiero dirigirme, entonces mejor hacer hincapié en el objetivo profesional, aunque podemos correr el riesgo de limitarnos o condicionarnos a unos determinados puestos de trabajo.

En definitiva, cada uno de nosotros deberá decidir qué le conviene más destacar: nuestros puntos fuertes, conocimientos, competencias, habilidades o nuestros intereses y motivaciones profesional

4. METODOLOGIA

La metodología propuesta tiene diferentes elementos que se vinculan y se retroalimentan, no necesariamente tienen un desarrollo secuencial. Los elementos son:

- Categorías temáticas
- Competencias en esas categorías
- Contenidos normalizados
- Evaluación (rúbricas)
- Metodologías de enseñanza
- Competencias en perfiles profesionales

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

Se busca generar el mapeo de los cursos a las competencias. En lo que sigue se va a bosquejar el desarrollo propuesto e instanciarlo en el área Documentación Digital.

Se busca establecer cuáles son las competencias fundamentales o nucleares, tomando encuéntralas unidades curriculares del área de DD. De estas unidades se extrajeron las grandes categorías temáticas o agrupación de contenidos medulares y desde allí las competencias que se buscan generar sobre esos contenidos. Estas competencias necesitan ser evaluadas a través de algún patrón que se diseñó como una rúbrica.

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

EJERCICIO DE SIMULACIÓN Y RESPUESTA A ATAQUES CIBERNÉTICOS

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

INTRODUCCIÓN

El aumento del uso de Internet en América Latina está ocurriendo a una de las tasas más altas del mundo Consecuentemente, ha habido una digitalización del riesgo corporativo. En los últimos años, ha sido tan dramático el cambio del valor de los activos corporativos que ahora casi el 90% de los activos corporativos son digitales. Como resultado, los responsables de las políticas, los reguladores, los accionistas y el público están más conscientes que nunca de los riesgos corporativos de ciberseguridad. Las organizaciones corren riesgos de pérdida de propiedad intelectual y sus planes comerciales, destrucción o alteración de datos, disminución de la confianza pública e interna de las partes interesadas, interrupción de la infraestructura crítica y evolución de las sanciones reglamentarias. Cada uno de estos riesgos puede afectar negativamente las posiciones competitivas, el precio de las acciones y el valor para los accionistas. Las compañías líderes perciben los riesgos cibernéticos de la misma manera como lo hacen con otros riesgos críticos: en términos de compensación de riesgo-recompensa. Esto es especialmente desafiante en el dominio cibernético por dos razones. Primero, la complejidad y persistencia de las amenazas cibernéticas ha crecido dramáticamente. Las corporaciones, incluso las empresas que son comparativamente pequeñas, ahora enfrentan eventos cada vez más sofisticados que logran sobrepasar las defensas tradicionales. Con el aumento de la complejidad de estos ataques, también aumenta el riesgo que representan para las organizaciones. Los efectos potenciales de una violación de los datos se están extendiendo mucho más allá de la pérdida, modificación o interrupción de la información. Los ataques cibernéticos pueden tener un impacto desastroso en la reputación y marca de una organización. Las empresas y los directores también pueden incurrir en riesgos legales y financieros derivados de los ciberataques A pesar de estos riesgos, la motivación para implementar tecnologías nuevas y emergentes para impulsar el desarrollo económico, reducir los costos, mejorar el servicio al cliente y estimular la innovación es más fuerte que nunca. A medida que crecen las amenazas de ciberseguridad, las Juntas Corporativas pueden ser proactivas en materia de ciberseguridad y dedicarse a realizar evaluaciones de riesgos y mantener un diálogo regular con la alta administración en toda la organización. Si no se abordan estas vulnerabilidades, los ciberdelincuentes pueden chantajear a las organizaciones con amenazas de divulgar información sobre sus vulnerabilidades, riesgos y secretos competitivos. Para las organizaciones, hay muchos otros beneficios de implementar medidas de ciberseguridad más robustas que la simple protección contra ataques.

Estos incluyen:

•Ventaja competitiva sobre compañías que tienen una seguridad menos sólida.
•Mejora de la eficacia en función de los costos, mediante protocolos eficaces de gestión de riesgos.
•Preservación de la reputación de la empresa.
•Contribución para mantener la integridad de la infraestructura general y proteger la confianza de los consumidores y de las partes interesadas internas.
•Demostración directa de la responsabilidad corporativa hacia todas las partes interesadas potencialmente afectadas, más allá de los clientes: empleados, accionistas, proveedores y la comunidad.
El Foro Económico Mundial informa que el rápido ritmo de la innovación y la conectividad de la red continuará aumentando en los próximos años, lo que hace que sea aún más crítico que se tomen medidas a nivel de la junta directiva en materia de ciberseguridad.
Manual de supervisión de riesgos cibernéticos para juntas corporativas
Estas presiones competitivas hacen que la supervisión concienzuda y exhaustiva a nivel de junta sea esencial. Las juntas deberán reconocer que la gestión y mitigación del impacto del riesgo cibernético requiere

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

un pensamiento estratégico que abarque más allá del departamento de TI. Un estudio de la Organización de los Estados Americanos y el Banco Interamericano de Desarrollo recomienda que, como mínimo, las juntas comprendan los riesgos cibernéticos a los que se enfrentan sus empresas, los principales métodos de ataque que podrían emplearse en su contra, y cómo su empresa gestiona y evalúa los problemas cibernéticos.

5. HIPOTESIS

¿Por qué nos atacarían?

Algunas organizaciones creen que es poco probable que sean víctimas de un ataque cibernético porque son de tamaño relativamente pequeño, no son una marca Conocida y/o no tienen cantidades sustanciales de datos confidenciales del consumidor, como números de
tarjetas de crédito o información médica. De hecho, los adversarios tienen en la mira a
organizaciones de todos los tamaños y de todas las industrias, buscando cualquier cosa que pueda ser de valor, incluidos los siguientes activos:

- Planes de negocios, incluidas las fusiones o estrategias de adquisición, ofertas, etc.;
- Algoritmos de negociación;
- Contratos o acuerdos propuestos con clientes, proveedores, distribuidores, socios de empresas conjuntas, etc.;
- Credenciales de inicio de sesión de los empleados y otra información útil;
- Información sobre las instalaciones, incluidos los
diseños de plantas y equipos, mapas de construcción y
planes futuros;
- Información de I + D, incluidos nuevos productos o servicios en desarrollo;
- Información sobre procesos de negocio clave;
- Código fuente;
- Listas de empleados, clientes, contratistas y proveedores;
- Datos del cliente, donante o fiduciario

6. OBJETIVO

General

Generar espacios que permitan realizar simulaciones en donde se logren identificar por donde se pueden hacer ataques cibernéticos en la institución.

7. METODOLOGIA

Para la E.S.E. Hospital Departamental San Vicente de Paul de Garzón, Los riesgos cibernéticos deben evaluarse de la misma manera en que una organización evalúa la seguridad física de sus activos humanos y físicos y los riesgos asociados con su posible compromiso. En otras palabras, la ciberseguridad es un problema de gestión de riesgos en toda la empresa que debe abordarse desde una perspectiva estratégica, económica, interdepartamental e interdivisional29. No es solo un problema de TI (o de tecnología), sino también de procesos de negocios, personas, datos o información, y valor. Por ejemplo, la ciberseguridad

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

debe incorporarse en los procesos y programas de recursos humanos a través de un enfoque que abarque toda la organización. Además, dado que las juntas en América Latina suelen estar integradas total o parcialmente por miembros de familia, es importante que las familias propietarias de las empresas estén debidamente informadas y sean conscientes de los problemas de ciberseguridad. La OEA y el BID han identificado que un gobierno corporativo maduro, en materia de ciberseguridad, requeriría un compromiso regular por parte de la junta y hacer ajustes rápidos y apropiados de la estrategia de ciberseguridad basados en amenazas y riesgos, así como realizar una asignación efectiva de fondos y atención en toda la organización para abordar las amenazas conocidas y desconocidas. El Foro Económico Mundial también hace hincapié en la necesidad de que las juntas directivas garanticen que la gerencia integre la resiliencia cibernética y la evaluación de riesgos en la estrategia comercial general y la gestión de riesgos en toda la empresa, así como la asignación de recursos y presupuestos.

8. CONCLUSION

La ciberseguridad no puede considerarse de forma aislada. Los miembros de la gerencia y la junta deben lograr el equilibrio adecuado entre proteger la seguridad de la E.S.E. y mitigar las pérdidas, al tiempo que continúan asegurando la rentabilidad y el
crecimiento en un entorno competitivo. Muchas innovaciones técnicas y prácticas comerciales que mejoran la rentabilidad también pueden socavar la seguridad. Por ejemplo, muchas tecnologías como la tecnología móvil, la computación en la nube y los dispositivos "inteligentes" pueden generar ahorros significativos en los costos y eficiencias empresariales, pero también pueden crear problemas de seguridad importantes si se implementan incorrectamente. Si se implementan correctamente, podrían aumentar la seguridad. De manera similar, las tendencias como traiga su propio dispositivo (BYOD, por sus siglas en inglés), el acceso a la información las 24 horas, los 7 días de la semana, el crecimiento de la analítica sofisticada de los "grandes datos" y el uso de largas cadenas de suministro internacionales pueden ser tan rentables que son elementos esenciales para que un negocio siga siendo competitivo. Sin embargo, estas prácticas también pueden debilitar dramáticamente la seguridad de la organización.
Las organizaciones se podrán defender mientras se mantengan competitivas y conserven la rentabilidad. Pero los métodos exitosos de ciberseguridad no pueden simplemente "añadirse" al final de los procesos de negocios. La ciberseguridad debe integrarse en los sistemas y procesos clave de una organización de principio a fin; y cuando se hace bien, puede apoyar en la construcción de una ventaja competitiva. Un estudio encontró que cuatro controles de seguridad básicos eran efectivos para prevenir el 85 por ciento de las intrusiones cibernéticas:

•Restricción de la instalación de aplicaciones por parte del usuario ("lista blanca").
•Asegurarse de que el sistema operativo esté "parchado" con actualizaciones actuales.
•Asegurar que las aplicaciones de software se actualicen regularmente.
•Restricción de los privilegios administrativos (es decir, la capacidad de instalar software o cambiar los ajustes de configuración de una computadora).

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

EVALUACIÓN DE VULNERABILIDADES INFORMÁTICAS

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

INTRODUCCIÓN

En la E.S.E. Hospital Departamental San Vicente de Paul. El avance tecnológico ha traído consigo un reto mayor para quienes se dedican al combate de programa con características maliciosas, la difusión de nuevas técnicas y metodologías de ataques y amenazas informáticas cada vez más sofisticadas y eficaces. No es un secreto la cantidad de recursos que invierten las organizaciones para evitar intrusiones y manipulaciones que pongan en riesgo, desde la integridad de la data hasta las operaciones propias de la entidad.

Hoy en día, las organizaciones son más dependientes de sus redes informáticas y un problema que las afecte, por pequeño que sea, puede llegar a comprometer la continuidad de las operaciones, situación que inevitablemente se traduce en pérdida económica, retraso en las operaciones y crisis de confianza por parte de los usuarios.

Aunado a lo anterior se encuentra la ausencia de una adecuada política de seguridad de las redes. Este es un problema que está presente por el sólo hecho de subestimarse las fallas que a nivel interno se producen, considerando sobre todo que la propia complejidad de la red es una dificultad para la detección y corrección de múltiples y variados problemas de seguridad que van siendo detectados por la E.S.E.

OBJETIVO

General

El objetivo del análisis de riesgo es identificar los riesgos basados en la identificación de los activos, de sus amenazas y vulnerabilidades.
Definición del alcance del modelo: el primer paso que se siguió de acuerdo a la metodología propuesta fue definir el alcance de esta evaluación de riesgo. El alcance de esta investigación son los activos que están en custodia de la Dirección de Servicios Telemáticos de la E.S.E. Hospital.

Específicos

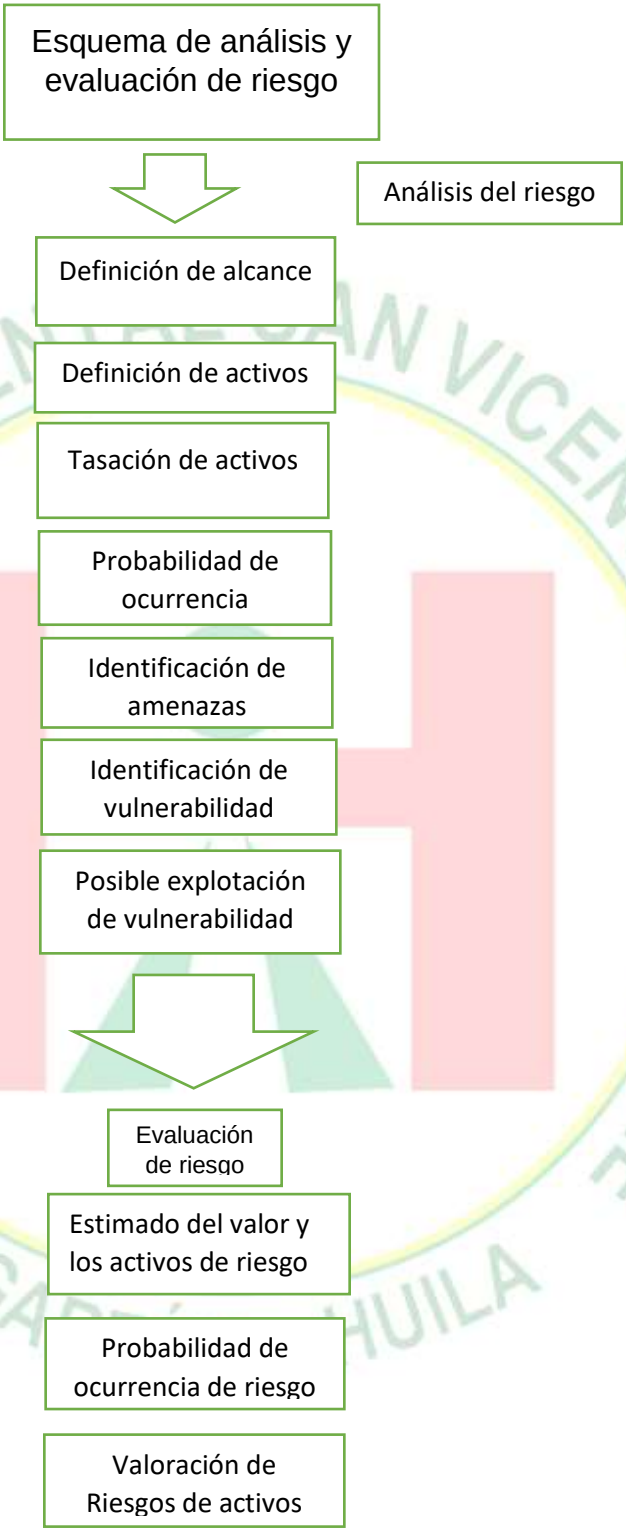
Identificación de activos: una vez definido el alcance se procedió a identificar los activos. Se identificaron 8 activos de información vitales

Activos de información (datos, de manuales de usuario, entre otros)

- Documentos en papel (contratos)
- Activos de software (aplicación, software de sistemas, entre otros)
- Activos físicos (computadoras, servidores, medios magnéticos, enrutadores, entre otros)
- Personal (estudiantes, clientes, empleados, entre otros)
- Imagen de la compañía y reputación
- Servicios (comunicaciones, entre otros)

METODOLOGIA

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).



Este estudio se plantea como la continuación de un trabajo el cual busca evaluar la seguridad de la información a la luz de los controles de la ISO.

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

Se busca evaluar los riesgos a los cuales pueden estar sometidos los activos de información que se encuentran en custodia en la DST. El desarrollo del mismo se llevó a cabo tres fases: la primera consistió en una investigación documental; la segunda en una investigación de campo y la tercera la conformó el análisis, evaluación y tratamiento del riesgo de los activos en custodia de la DST. Siempre en el contexto de un estudio de caso.

Conocer el riesgo a los que están sometidos los activos es imprescindible para poder gestionarlos, y por ello han surgido una multitud de guías informales, aproximaciones metódicas y herramientas de soporte las cuales buscan objetivar el análisis para saber cuán seguros (o inseguros) están dichos activos y no llamarse a engaño (MAGERIT, 2005).

CONCLUSION

Para la E.S.E. Hospital Departamental San Vicente de Paul, Es de suma importancia que el proceso de evaluación del riesgo permite a una organización alcanzar los requerimientos del estándar. Este proceso ayuda a cualquier organización que desee establecer un Sistema de Gestión de la Seguridad de la Información (SGSI) en concordancia con la cláusula 4.2.1 de la norma.

La evaluación de riesgo es el proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado de importancia del riesgo. El objetivo de esta evaluación es la de identificar y evaluar los riesgos. Los riesgos son calculados por una combinación de valores de activos y niveles de requerimientos de seguridad de la E.S.E.

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

CONTROL DE CAMBIOS

El control de cambios, describe las modificaciones realizadas al presente Manual de Procedimientos y define la nueva versión que se genera por cambios de fondo requeridos.

FECHA	CAMBIO	NUEVA VERSIÓN	ELABORÓ

GENERALIDADES SEGURIDAD DIGITAL		
Elaborado o Actualizado por: JORGE HUMBERTO GONZALEZ MENESES	**Revisado por:** ESPERANZA FIERRO VANEGAS	**Aprobado por:** JORGE HUMBERTO GONZALEZ BAHAMON
Cargo: COORDINADOR UNIDAD FUNCIONAL SISTEMAS DE INFORMACIÓN	**Cargo:** SUBDIRECTORA ADMINISTRATIVA	**Cargo:** GERENTE
Adopción Resolución Institucional Nº 0975 DE 14 DE DICIEMBRE 2021: aspectos generales del sistema de información (gobierno y seguridad digital) de la unidad funcional sistemas de información.		

Calle 7 No. 14-69 PBX (098) 8332441 Ext: 256 Fax (098) 8333225 Gerencia (098) 8332570
web: www.hospitalgarzon.gov.co – Email: calidad@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).