IDENTIFICACION DE LOS PRINCIPALES RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, A LOS CUALES SE ENCUENTRAN EXPUESTAS LAS ENTIDADES QUE HACEN PARTE DE LA RED DE PRESTACION DE SERVICIOS DE SALUD DEL DISTRITO CAPITAL

EDWIN GIOVVANI VASQUEZ PULECIO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2021

IDENTIFICACION DE LOS PRINCIPALES RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, A LOS CUALES SE ENCUENTRAN EXPUESTAS LAS ENTIDADES QUE HACEN PARTE DE LA RED DE PRESTACION DE SERVICIOS DE SALUD DEL DISTRITO CAPITAL

EDWIN GIOVVANI VASQUEZ PULECIO

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

TUTOR
LUIS FERNANDO BARAJAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Con amor dedico éste trabajo a mi Esposa e Hija, quienes me apoyaron en todo momento de manera incondicional, a mis padres quienes me inculcaron la necesidad de estudiar y superarme.

AGRADECIMIENTOS

Agradezco a los docentes de la Universidad Nacional Abierta y a Distancia UNAD, de quienes obtuve los conocimientos necesarios para culminar mis estudios, por el esfuerzo realizado en el énfasis de impartir conocimiento de manera reiterativa, para lograr mejores personas y más capaces.

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

LISTA DE ANEXOS

GLOSARIO

AMENAZA: Evento desfavorable que puede ocurrir generando consecuencias negativas sobre los activos de información, provocando indisponibilidad, perdida de información, funcionamiento incorrecto.

ANTIVIRUS: Programa informático diseñado específicamente para detectar, bloquear, desinfectar o eliminar código malicioso (Troyanos, Virus, Gusanos, etc).

AUTENTICACION: Proceso de comprobación de usuario autorizado al acceder a un equipo de cómputo o servicio.

BACKUP: Copia de seguridad a ficheros, bases de datos, o aplicaciones en un activo de información: este proceso suele realizarse en dispositivos externos (Discos Duros, Memorias USB, CD/DVD, etc).

BIOMETRIA: Método de reconocimiento de usuarios y/o personas, el cual se basa en características fisiológicas (Retina, Rostro, Iris, Huella Dactilar).

BOTNET: Conjunto de ordenadores controlados remotamente por un atacante con el fin de realizar actividades maliciosas.

BUG: Error o falla en un programa en un dispositivo o sistema que genera un resultado no deseado.

CERTIFICADO DIGITAL: Fichero informático generado por una entidad certificadora que asocia los datos de una persona, organización o empresa con el fin de confirmar su identidad digital en internet.

CLOUD COMPUTING: Permitir a los usuarios almacenar información en servidores de terceros, para consultar desde cualquier equipo de cómputo(Terminal) con acceso a la red.

CONFIDENCIALIDAD: Propiedad de la información que garantiza el acceso único a personal autorizado.

CORTAFUEGOS: Sistema de seguridad compuesto por programas o dispositivos de Hardware, los cuales se encuentran en el límite de la red con el objetivo de permitir o denegar el flujo de tráfico entre diferentes ámbitos, con el fin de proteger y asegurar las comunicaciones entre la red y el internet.

CRIPTOGRAFIA: Técnica que consiste en cifrar un mensaje, en el proceso un texto legible al cifrarse se convierte en texto ilegible. Existen dos tipos principales, cifrado simétrico y asimétrico o de clave pública.

DENEGACION DE SERVICIO: Conjunto de técnicas cuyo objetivo es el de generar indisponibilidad a un servidor, sobrecargándolo para que de esta forma los usuarios legítimos no puedan acceder a los servicios prestados por este servidor.

DIRECCION IP: Corresponde a un número único que identifica a un dispositivo en la red, dependiendo de la configuración se registra de manera fija en cada dispositivo o de manera automática (DHCP)

DIRECCION MAC: También conocida como dirección física, corresponde a un valor de 48 bits único e irrepetible que identifica a cada equipo conectado en la red. Esta dirección es escrita en forma binaria al momento de su fabricación.

DISPONIBILIDAD: Corresponde a la capacidad de un sistema de información o un servicio en ser accesible y utilizable por procesos o usuarios autorizados. Hace

parte de las tres dimensiones de la seguridad de la información junto con la Confidencialidad e Integridad.

DNS: Se refiere al servicio de definición de nombres de dominio, la función principal es de traducir direcciones IP en los nombres de Dominio.

EXPLOIT: Secuencia de comandos utilizados para aprovechar un fallo o vulnerabilidad de un sistema y así provocar un error o imprevisto.

FIRMA ELECTRONICA: Define el conjunto de datos electrónicos, asociados a un documento electrónico. Se consigue calculando el valor Hash del documento para así proceder a cifrarlo con clave pública del destinatario.

FUGA DE DATOS: Se hace referencia a la perdida de confidencialidad de la información privada de una empresa o persona.

GUSANO: Programa malicioso (Malware), con la propiedad de propagarse rápidamente, replicándose a nuevos sistemas con el fin de infectarlos utilizando cualquier tipo de medio de transmisión (Correo, chat P2P, etc)

HTTP: Protocolo de transferencia de Hipertexto, es el protocolo más utilizado para la navegación web, utiliza el esquema de petición/respuesta, la información se envía en texto claro lo que quiere decir que o cuenta con ningún tipo de cifrado.

HTTPS: Protocolo seguro de transferencia de Hipertexto, el cual en su trasmisión de datos utiliza un algoritmo de cifrado simétrico, es utilizado por entidades que utilizan datos personales o claves, bancos o tiendas con pagos en línea.

INCIDENTE DE SEGURIDAD: Cualquier suceso que afecte la información o la disponibilidad de los servicios de la empresa.

INTEGRIDAD: Propiedad de la información que garantiza la exactitud de los datos almacenados o transportados asegurando que no se presente alteración, destrucción o perdida de los datos.

INYECCION SQL: Tipo de ataque que de acuerdo a una vulnerabilidad encontrada se aprovecha para inyectar código que permita la obtención de datos de manera ilegítima.

IPS: Sistema de prevención de Intrusos, que se utiliza para proteger al sistema de ataques la cual hace parte de una extensión IDS, aunque es más acercada al Firewall.

LAN: Red de área local, de pequeña amplitud que se limita a oficinas, viviendas o edificios, con el fin de interconectar dispositivos, impresoras, servidores, etc.

MALWARE: Tipo de software con el objetivo de infiltrarse en el sistema de información para dañar los datos del usuario

METADATOS: Conjunto de datos relacionados con un documento, tomando información descriptiva, de administración y gestión del mismo.

NO REPUDIO: Envió de información a través de la red con la capacidad de demostrar la identidad del emisor.

PARCHE DE SEGURIDAD: Conjunto de cambios y mejoras que se aplican a un software para corregir errores de seguridad en sistemas operativos o programas.

PENTEST: Corresponde a una prueba de penetración a un sistema de hardware o software, con el objetivo de hallar vulnerabilidades.

PHARMING: Ataque informático con el fin de aprovechar vulnerabilidades en servidores DNS.

PHISHING: Estafa cometida a través de medios electrónicos, donde el estafador consigue información confidencial de usuarios legítimos (Contraseñas, acceso a bancos, etc)

PLAN DE CONTINGENCIA: Consiste en una estrategia planificada por un conjunto de recursos que permitan realizar un respaldo ante una emergencia, encaminado a conseguir una restauración de los servicios de manera progresiva y ordenada.

POLITICA DE SEGURIDAD: Medidas de seguridad que una empresa decide tomar luego de evaluar el valor de sus activos y los riesgos a los cuales se encuentran expuestos.

PROTOCOLO: Reglas o estándares que definen la sincronización de la comunicación.

PUERTA TRASERA: Hace referencia a cualquier punto débil de un sistema informático por el cual una persona no autorizada pueda acceder.

RANSOMWARE: Un atacante toma control de un equipo infectado, secuestrando la información, cifrándola para que permanezca ilegible, con el fin de extorsionar al usuario solicitando un rescate a cambio de dinero.

RED PRIVADA VIRTUAL: Permite una extensión segura de la red de área local LAN, sobre una red pública o no controlada.

ROUTER: Dispositivo encargado de distribuir tráfico en la red a partir del prestador de servicio de internet y la red interna.

SERVIDOR: Equipo cuyo propósito es el de prestar un servicio para la gestión de Software, pueden prestar servicios de alojamiento de información, de aplicativos web o cliente/servidor, de mensajería etc.

SNIFFER: Programa encargado de monitorizar la información que circula por la red con el fin de capturar información para ser analizada.

SPOOFING: Técnica de suplantación de identidad llevada a cabo por un atacante haciendo uso de malware poniendo en riesgo la privacidad de los usuarios.

SPYWARE: Es un tipo de malware que captura información de un ordenador y la envía a otra ubicación remota sin el consentimiento del usuario.

SUPLANTACION DE IDENTIDAD: Actividad maliciosa en donde el atacante se hace pasar por otra persona con el objetivo de cometer un tipo de fraude o acoso.

TROYANO: Tipo de malware o software malicioso con la capacidad de auto replicación, requiere uso de ingeniería social para su replicación.

URL: Hace referencia una dirección que identifica un lugar en internet.

VIRTUALIZACION: Medio para crear una versión virtual de un recurso o dispositivo ya sea un servidor con el apoyo de un software.

VIRUS: Programa diseñado para que al momento de ejecutarse se copie e si mismo, sus efectos son variables los cuales pueden borrar información, enviar información, ralentizar sistemas operativos etc.

VLAN: Red de área Virtual, independiente dentro de una red física configurada mediante software.

VULNERABILIDAD: Deficiencias o fallos en un sistema o programa que permite a usuarios no autorizados acceder a información, llevar a cabo operaciones no permitidas.

WIFI: Red de dispositivos inalámbricos interconectados con acceso a internet, el cual no utiliza cable físico para enviar información

ZERO-DAY: vulnerabilidad en sistema conocida por determinados atacantes y son desconocidas por los fabricantes en donde no existe un parche de seguridad para dar solución.

RESUMEN

Con la implementación de historia clínica digital en las entidades de salud, se hace necesario realizar todos los procesos que conlleven a garantizar la seguridad de los datos asociados a atenciones de salud, adoptar las medidas y recomendaciones para impedir la violación de la privacidad de la información que en la mayoría de ocasiones son producto de descuido, exceso de confianza o errores por parte de sus mismos funcionarios (Personal de TIC's, Personal Médico-Asistencial, Personal Administrativo). En este trabajo se presenta un análisis de seguridad de la información enfocado en la en la gestión de vulnerabilidades, riesgos y optimización de los activos de información de entidades prestadoras de servicios de sector salud en el distrito capital, se recopilara la información existente que hace énfasis en la seguridad de la información la cual aportara al enfoque que tienen estas entidades con respecto a proteger los activos de información, se realizan entrevistas al personal encargado de las tecnologías de la información con el fin de conocer cómo se realiza la protección y control de la información. Con el levantamiento de información actual, se realizarán sugerencias e indicaciones necesarias que se deben optar, teniendo en cuenta que los recursos en entidades del estado son limitados frente a inversiones tecnológica. Es así que la implementación de dichos controles debe tener un complemento adicional de bajo costo.

ABSTRACT

With the implementation of digital medical records in health entities, it is necessary to carry out all the processes that lead to guaranteeing the security of the data associated with health care, adopting the measures and recommendations to prevent the violation of the privacy of the information which in most cases are the product of carelessness, overconfidence or errors on the part of their own officials (ICT Staff, Medical-Assistance Staff, Administrative Staff). This paper presents an information security analysis focused on the management of vulnerabilities, risks and optimization of the information assets of entities that provide health services in the capital district, the existing information that emphasizes In information security, which will contribute to the approach that these entities have with respect to protecting information assets, the necessary investigations will be carried out supported by interviews with the personnel in charge of information technologies in order to know how the protection and control of information. With the current information gathering, suggestions and necessary indications will be made that must be chosen, taking into account that the resources in state entities are limited compared to technological investments. Thus, the implementation of these controls must have an additional low-cost complement.

INTRODUCCIÓN

Garantizar la seguridad de la información, tiene como base la implementación de controles, procesos, procedimientos basados en estándares definidos de acuerdo a las mejores prácticas que permitan realizar diagnósticos, planificar, implementar y hacer mejoramiento continuo. Estos en su defecto hacen parte de un modelo de seguridad y privacidad de la información, la cual se encuentra enfocada a los procesos misionales y tamaño de la infraestructura de la entidad.

Es por ello que la seguridad de la información en entidades de prestación de servicios salud debe hacer énfasis en la protección no solamente del dato, sino en la representación que este hace a un paciente. Así que la importancia de realizar un análisis enfocado en los principales riesgos de seguridad de la información en entidades que hacen parte de la red de prestación de servicios de salud, identificando las dificultades en proceso de gestión y mitigación de riesgos, ya que la falta de controles ahonda las dificultades propias que se puedan presentar debido a una mala administración de los activos de información. Se hace indispensable revisar las políticas de seguridad de la información, modificarlas, ajustarlas, implementarlas y hacer el análisis correspondiente a fin de tomar las medidas necesarias que impliquen la mitigación del riesgo, teniendo en cuenta el no afectar el flujo normal de los procesos en la entidad, ya que se deben garantizar los medios para la atención de los pacientes.

Las normas, herramientas y procedimientos enfocados en la seguridad de la información, tienen como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información, es por ello que el área de TIC, debe implementar todos aquellos modelos de seguridad que permitan la continuidad del negocio.

1. DEFINICIÓN DEL PROBLEMA

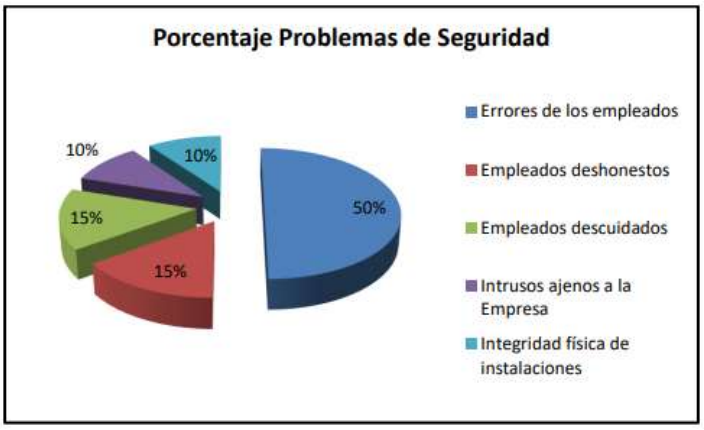
1.1 ANTECEDENTES DEL PROBLEMA

Dentro de las consultas realizadas, se encuentran avances relacionados a la seguridad de la información en entidades de salud, enfocados a vulnerabilidades en las historias clínicas digitales asociadas a errores o fallas cometidas por el personal que labora en entidades de salud[1].

Según la revista empresarial, los ataques cibernéticos dirigidos a proveedores de atención medica aumentaron en un 63% en el año 2016[2].

Dentro de las políticas de seguridad informática del hospital departamental universitario del Quindío se indican los estudios realizados que muestran el porcentaje de problemas de seguridad en sistemas basados en redes, como se ilustra en la figura 1

Figura 1. Porcentaje Problemas de Seguridad



Fuente: https://hospitalquindio.gov.co/hospital/documentos/PoliticasDeSeguridad/politicas_seguridad.pdf

[1] ACHURY, N. (2018). VULNERABILIDADES DE LAS HISTORIAS CLÍNICAS DIGITALES OCASIONADAS POR LOS TRABAJADORES DE SALUD. CONSULTADO EL 28 NOVEMBER 2020, DISPONIBLE EN: HTTPS://REPOSITORY.UNAD.EDU.CO/BITSTREAM/HANDLE/10596/25666/%20NAACHURYP.PDF?SEQUENCE=1

[2] BIDDLE, S. (2020). Ciberseguridad en el Sector de Salud. [Consultado el 28 de Noviembre de 2020]. Disponible en: https://revistaempresarial.com/salud/salud-ocupacional/ciberseguridad-sector-salud/

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo realizar un análisis a la seguridad de la información para entidades que hacen parte de prestación de servicios de salud en el distrito capital, que permita conocer las causas y/o dificultades frente a la prevención de vulnerabilidades, mitigar riesgos y optimizar la gestión de activos de información?

2 JUSTIFICACIÓN

Los avances en materia de prestación de servicios en una entidad de salud, implica la necesidad de aumento de infraestructura, para garantizar el acceso a las aplicaciones de uso de registro y consulta de información administrativa y asistencial. Es por ello que se hace necesario implementar las recomendaciones necesarias para garantizar la seguridad de la información de la entidad.

El análisis de seguridad de la información en entidades que hacen parte de la red de prestación de servicios de salud en el distrito capital, hace énfasis en la identificación de vulnerabilidades y riesgos en la seguridad de la información, basado en diagnósticos, con el fin de identificar posibles implementaciones de controles de mitigación que permitan el control eficiente en los flujos de información. Garantizando los pilares de la seguridad en la información (Confidencialidad, Integridad y Disponibilidad), teniendo en cuenta además que la información almacenada en estas instituciones corresponde en su mayoría a Historias Clínicas, las cuales se encuentran clasificadas como documentos privados y de manejo especial.

Dentro del análisis general, se tomaron en cuenta las vulnerabilidades en servidores, equipos de transmisión de datos (Switch, Router, Firewall, Access Point, etc.), gabinetes, centros de cómputo, equipos de cómputo de usuario final y demás componentes que intervienen en el flujo de información. Gracias a este análisis se

identificaron las fallas propias en la gestión de procesos, administración de dispositivos y falta de controles de seguridad.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Elaborar un análisis de seguridad de la información de los principales riesgos de seguridad de información en las entidades que hacen parte de la red de prestación de servicios de salud en el distrito capital.

3.2 OBJETIVOS ESPECÍFICOS

- Evaluar de acuerdo con su criticidad, los principales riesgos de seguridad de la información que afrontan las entidades que pertenecen a la red de prestación de servicios de salud en el distrito capital

- Justificar la necesidad de implementar acciones, procesos y procedimientos, enfocados a la seguridad de la información.

- Recomendar al personal encargado de TIC, de acuerdo con el análisis realizado, los procedimientos y mecanismos que permitan la mitigación de riesgos y vulnerabilidades.

- Diseñar una matriz de Vulnerabilidades que apoye la creación de un modelo de políticas de Seguridad.

4 MARCO REFERENCIAL

La información contenida en la historia, es un registro obligatorio de las condiciones de salud de un paciente. Este documento es privado el cual contiene lo detalles íntimos relacionados con aspectos físicos, sociales y psíquicos, registrados con los actos médicos y demás procedimientos realizados por el equipo de salud de manera cronológica. De esta manera con el fin de garantizar su integridad, confidencialidad y disponibilidad, se deben implementar los mecanismos necesarios que impliquen la seguridad de la información asistencial y administrativa de la institución, teniendo en cuenta además la gran cantidad de funcionarios, (Personal asistencial y administrativo), que tienen acceso a esta información, es importante hacer énfasis en el especial cuidado frente a la correcta capacitación y exigencia a los protocolos al personal que registra y consulta información en los diferentes medios de registro de historia clínica, no sin antes realizar un control por parte de los administradores del sistema, quienes crean los perfiles de acuerdo a las necesidades de cada usuario, así mismo hacer los controles necesarios a los dispositivos de terceros (Equipos de personal médico). Todo ello con el fin de garantizar que no se generen fugas de información o uso indebido de los mismos.

Las entidades enfocadas en el sector salud pueden destacarse por ser un blanco para el ataque de cibercriminales, ya que este sector cumple con el rol de bienestar y salud en la sociedad. La información privada y personal contenida en la historia clínica, en manos indebidas, puede derivar en extorsión a pacientes o funcionarios.

Dentro de la información almacenada en una entidad del sector salud, no solamente se hace énfasis en registros clínicos de pacientes, además se registra información financiera, valores de pagos de honorarios al personal contratado, contratos vigentes con otras entidades, investigaciones médicas, resultados de procesos relacionados con nuevos tratamientos o medicamentos, información genética. Etc.

4.1 MARCO TEÓRICO

La implementación de un sistema de seguridad de la información, debe contener los aspectos básicos, enfocados en metodologías y estándares de protección como ISO/IEC 27000, Ethical Hacking, OSSTMM, etc, que permitan garantizar y en lo posible certificar un sistema seguro, protegido y confiable.

4.1.1 Sistema de Gestión de Seguridad de la Información. Responde a una política apoyada en normas y procesos de manera estratégica, donde su objetivo es el de asegurar la continuidad del negocio apoyado en la ejecución de buenas prácticas, con el fin de mitigar riesgos y reducir al mínimo los daños que se presenten gracias a una contingencia y de esta manera se tomen decisiones que permitan optimizar el correcto resguardo de la información.

4.1.1.2 Políticas de Seguridad. Responden a la necesidad de mantener un sistema seguro, las cuales se implementan mediante procedimientos asociados a la administración y uso, con el fin de identificar y evaluar riesgos y realizar las acciones necesarias. Los procesos y procedimientos embebidos en las políticas de seguridad, se deben poner en práctica por todo el personal ya sea usuarios, administradores en donde se definan responsables ante una situación presentada.

4.1.1.3 Modelo PHVA. Se determina el procedimiento de acuerdo a la definición de un alcance sistémico, al identificar y evaluar un riesgo, definición de políticas, tratamiento del riesgo, objetivos de control, aplicabilidad y aprobación por parte de la gerencia. Este modelo de diagnóstico se representa mediante la figura 2

Figura 2. Modelo de seguridad y Privacidad de la Información

Fuente: MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION (2016) [Consultado el 21 de Octubre de 2020]. https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

4.1.1.4 Planeación de Seguridad en la Red. Las estrategias definidas en la organización, deben ser comunicadas a todo su personal junto con la importancia de contar con un sistema de información seguro, donde se promueva la cultura de seguridad, es así que no solo con la creación de políticas de seguridad se garantice un sistema seguro, si los responsables no se apropian de manera responsable.

4.1.1.5 Vulnerabilidades. Hace referencia a la debilidad encontrada en un sistema informático, el cual permite a un atacante acceder de manera abusiva, violando el acceso y consistencia del sistema, de sus aplicaciones o sus datos almacenados

4.1.1.6 Ataques. Corresponde a un intento organizado con el fin de cometer un daño a un sistema, esta acción es cometida generalmente por un hacker o pirata informático

4.2 MARCO CONCEPTUAL

El análisis de riesgo es un proceso cuantitativo y cualitativo que permite identificar todo aquello que se considere como amenaza o vulnerabilidad tanto para el hardware como para el software.

Las vulnerabilidades en un sistema hacen referencia a las debilidades, las cuales pueden ser utilizadas por un tercero para hacer algún tipo de daño. El uso de software desactualizado o implementaciones no compatibles generadas, gracias a falta de presupuesto, expone un escenario preocupante ya que, por ejemplo; el no actualizar a sistemas operativos con soporte vigente (Windows 7 o anteriores) implica una exposición a ataques Ransomware.

La integración de dispositivos médicos que se conectan a internet con la finalidad de brindar información remota del estado de salud de los pacientes, implica un reto adicional a las necesidades de protección de datos, debido a lo que esto representa frente a la vulnerabilidad ante ataques informáticos a los dispositivos del usuario final

Gestión del Riesgo: Aquí se debe Determinar, clasificar, analizar, y valorar la exposición de la información, utilizando diferentes métodos que permitan identificarlos, para así implementar medidas de seguridad que permitan mitigar los hallazgos en cada uno de los procesos identificados.

Gestión de Seguridad de la información: Los administradores de TIC, realizan un conjunto de procesos apoyados en normas vigentes, e implementación de políticas de seguridad, con el fin de asegurar la información y mantener la integridad, confidencialidad y disponibilidad.

Ciclo de mejora continua: Todos aquellos responsables de la seguridad de la información se enfocan en Panificar (Establecer objetivos e identificación de procesos), Hacer (Implementación de Acciones necesarias y cambios), Verificar (Periodos de Pruebas y planes de mejoras), Actuar (Realizar las mediciones y

modificaciones necesarias.)[3]

Medidas de seguridad: Los administradores involucrados en la seguridad de la información se enfocan en los procesos que implican la mitigación de riesgos, minimizando vulnerabilidades, gracias a los análisis en los distintos sistemas de información y de esta manera salvaguardando la información.

Infraestructura: Los administradores de seguridad de la información deben realizan el análisis al conjunto de elementos de Hardware y Software que se encuentran asociados a los activos de información, que hacen uso de una red de transmisión de datos, con el fin de identificar vulnerabilidades físicas y lógicas

Dentro de las entidades que hacen parte del sector salud del distrito capital, se emplean diferentes sistemas dispersos que requieren conectividad entre sí, debido a los contratos entre diferentes prestadores de servicios de salud. En estas entidades suele contratarse servicios de radiología, laboratorio clínico u otros proveedores que cuentan con su propio software de gestión. Esto implica la necesidad de interconectar sistemas (interfaz), para la transmisión de datos, lo cual genera una importante exposición a la información. Es allí donde se deben implementar los procesos, protocolos y procedimientos descritos dentro de las políticas de seguridad de la información que garanticen fluidez y la no fuga de información

Las áreas principales a las cuales se encuentra enfocada la seguridad de la información corresponden a:

[3] VEGA VELASCO, W. (2008). Políticas y Seguridad de la información. [Consultado el 28 de Octubre de 2020].,, Disponible en:http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008#:~:text=Las%20pol%C3%ADticas%20de%20seguridad%20se,y%20disponibilidad%20de%20la%20informaci%C3%B3n.

- Confidencialidad: Acceso a usuarios autorizados.
- Integridad: Completitud, integralidad y coherencia de los datos
- Disponibilidad: La información se debe encontrar disponible cada vez que el usuario lo requiera.
- Autenticación: Capacidad de demostrar si un usuario o aplicación si corresponde.

4.3 MARCO HISTÓRICO

La ciberseguridad a través de la historia se encuentra asociada al factor humano y su evolución, es así como se crea desde la antigüedad la creación de estrategias que permitan la continuidad, ya sea de supervivencia, negocio, acción o ciclo de vida. Ante las adversidades se generan herramientas de protección que aseguren el entorno ante cualquier riesgo o peligro. Es así que la seguridad ha evolucionado, en donde se aplica a seguridad física, laboral, económica, etc. La ciberseguridad hace referencia al tratamiento de riesgos, vulnerabilidades y amenazas, las cuales se aplican a cualquier entidad o de uso personal.

La migración de la historia clínica a formato digital se ha enfrentado a diferentes intentos de reforma:

- Antes de 1975 las demandas sanitarias eran atendidas por un conjunto desarticulado de instituciones de salud.
- La ley 10 de 1990, desmonto el sistema estatal y fortaleció financieramente el sector, preparando a los hospitales para acceder a recursos mediante venta de servicios.
- La ley 100 de 993 creo el sistema general de seguridad social, implantando la competencia regulada y el pluralismo estructurado

- En 2011 se expide la ley 1438, con el fin de mejorar el flujo de recursos en el sistema, dentro de esta se ordena la digitalización de las historias clínicas para el año 2013.
- Acuerdo 641 de 2016, expedido por el concejo de Bogotá D.C, donde se efectúa la reorganización del sector salud en el distrito capital. Fusión de los hospitales.

4.4 ANTECEDENTES O ESTADO ACTUAL

La seguridad tiene como origen la necesidad de proteger todo aquel activo para el uso y administración de la información, la cual ahora se encuentra digitalizada o almacenada de manera electrónica, antiguamente esta información se encontraba almacenada en medios físicos (Papel), así la seguridad se limitaba a controles de acceso al lugar donde se almacenaban estos documentos.

Las normas actuales de la serie ISO27000, se encargan de la estandarización, las cuales se generaron bajo la norma británica BS7799 en 1995, como guía de buenas prácticas y el sistema de gestión de seguridad en la información SGSI.[4]

Las entidades del sector salud realizan implementaciones de seguridad de la información con el fin de garantizar por le menos la integridad, confidencialidad y disponibilidad de la información, de acuerdo al levantamiento de información en una entidad de salud mediante realización de encuestas, se cuenta con la documentación de políticas, procesos y procedimientos asociados a la seguridad informática.

[4] ISOTOOLS. ¿En qué consiste el ciclo PHVA de mejora continua? (2020). [Consultado el 10 de Octubre de 2020]. Disponible en: https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/

4.5 MARCO LEGAL

Debido a que los ataques informáticos son cada vez más recurrentes en Colombia, se hace necesario reconocer los mecanismos legales vigentes en relación a la seguridad informática.

Ley 1581 de 2012. Dicta disposición sobre la protección de datos personales. Teniendo en cuenta que la información contenida en historia clínica en privada.

Ley 1266 de 2008. Se dictan disposiciones de Habeas Data, se regula el manejo de la información contenida en bases de datos. Ya que toda información contenida en bases de datos, es un derecho fundamental donde cualquier persona tiene derecho a solicitar información sobre si misma.

Ley 1273 de 2009. Capitulo1: Atentados contra la confidencialidad, integridad y disponibilidad de los datos de los sistemas informáticos. Capitulo2: Atentados informáticos y otras infracciones, asociados a ISO27000

Acuerdo 641 de 2016, en donde se efectúa la reorganización del sector salud de Bogotá D.C., definiendo las entidades que lo conforman, determinando la fusión de algunas entidades y creación de otras.[5]

Fusión de empresas sociales del estado.
Empresas Sociales del Estado de: Usme, Nazareth, Vista Hermosa, Tunjuelito, Meissen y El Tunal se fusionan en la Empresa Social del Estado denominada “Subred Integrada de Servicios de Salud Sur E.S.E.”

1.1 [5] ACUERDO 641 DE 2016. (2016). CONSULTADO EL 28 OCTOBER 2020, DISPONIBLE EN: HTTP://WWW.SALUDCAPITAL.GOV.CO/DOCUMENTS/ACUERDO_641_DE_2016.PDF

Empresas Sociales del Estado de: Pablo VI Bosa, del Sur, Bosa, Fontibón y Occidente de Kennedy se fusionan en la Empresa Social del Estado denominada "Subred Integrada de Servicios de Salud Sur Occidente E.S.E."

Empresas Sociales del Estado de: Usaquén, Chapinero, Suba, Engativá y Simón Bolívar se fusionan en la Empresa Social del Estado denominada "Subred Integrada de Servicios de Salud Norte E.S.E."

Empresas Sociales del Estado de: Rafael Uribe, San Cristóbal, Centro Oriente, San Blas, La Victoria y Santa Clara se fusionan en la Empresa Social del Estado denominada "Subred Integrada de Servicios de Salud Centro Oriente E.S.E."

Estas entidades deben contar son los siguientes principios:

- Auto sostenibilidad
- Transparencia

Según resolución 1995 de 1999. La historia clínica es un registro obligatorio, donde se consignan las condiciones de salud de un paciente, el cual se clasifica como documento privado, el cual se somete a terceros previa autorización del paciente.[6]

El contexto institucional en el cual se desarrollan los sistemas de información de salud en Colombia, Ley 100 de 1993 el cual reformo el sector salud, dentro de sus fundamentos y características del sistema se establece:

- Protección Integral: Brindar atención integral en la población en sus fases de información, educación y fomento de la salud, diagnostico, prevención, rehabilitación y tratamiento en oportunidad, cantidad y eficiencia.

[6] RESOLUCION NUMERO 1995 DE 1999. (1999). [Consultado el 20 de Octubre de 2020]. Disponible en: https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf

A partir del año 1993 se establece la función de informar el funcionamiento del sistema, relacionada con la salud de la población, indicadores de precios, gestión y calidad.

En el consejo privado de competitividad en 2010, se refieren las estrategias para fortalecer la institucionalidad de las estrategias TIC, entre otras:

- Aumentar la asignación de recursos para acceso y uso de TIC, facilitando su asequibilidad.
- Digitalizar la totalidad de las historias clínicas y desarrollar plataformas electrónicas para así facilitar el acceso y uso en línea.
- Identificar zonas de difícil acceso, con el fin de realizar telemedicina.

La ley 1438 de 2011 en la búsqueda de reformar el sistema general de seguridad social, en cuanto a información se establece responsabilidad al Ministerio de Protección Social estableciendo indicadores de desempeño implementando la plataforma SISPRO, aplicación web en donde se integran los sistemas de Registraduria Nacional, Ministerio de Hacienda, Dirección de Aduanas e Impuestos Nacionales - DIAN, el Sisben y las EPS.
En esta ley se define la obligatoriedad de digitalizar todas las historias clínicas a partir de diciembre de 2013.[7]

La conectividad de instituciones vinculadas al sector salud garantizaran antes de tres años la entrada en vigencia de la ley. El reporte de información es obligatorio para todos los actores del sistema los cuales se someten a sanciones por incumplimiento.

[7] BERNAL, O., 2011. Sistemas De Información En El Sector Salud En Colombia. [online] Scielo.org.co. [Consultado el 30 de Noviembre de 2020]. Disponible en: http://www.scielo.org.co/pdf/rgps/v10n21/v10n21a06.pdf

El desarrollo de sistemas e información en la salud se soporta en la definición de roles bajo las leyes actuales que corresponden sino también sobre el fomento del uso de tecnologías de información.[8]

5 DISEÑO METODOLÓGICO

Los aspectos metodológicos describen el proceso realizado para la preparación de instrumentos en la recolección de información y su correspondiente tabulación, los cuales se realizan de acuerdo a las siguientes fases:

- FASE 1: Evaluar de acuerdo con su criticidad, los principales riesgos de seguridad de la información que afrontan las entidades que pertenecen a la red de prestación de servicios de salud en el distrito capital
- FASE 2: Justificar la necesidad de implementar acciones, procesos y procedimientos, enfocados a la seguridad de la información
- FASE 3: Recomendar al personal encargado de TIC, de acuerdo con el análisis realizado, los procedimientos y mecanismos que permitan la mitigación de riesgos y vulnerabilidades.
- FASE 4: Diseñar una matriz de Vulnerabilidades que apoye la creación de un modelo de políticas de Seguridad.

5.1 PERSPECTIVA. De manera cualitativa se busca ahondar en los factores más relevantes asociados a la seguridad de la información en las entidades prestadoras de salud del distrito capital. De esta manera se considera la situación actual en términos de riesgos, vulnerabilidades y procesos de gestión de la información y mitigación de riesgos.

5.2 INSTRUMENTO DE ANALISIS.

[8] BERNAL, O., 2011. Sistemas De Información En El Sector Salud En Colombia. [online] Scielo.org.co. [Consultado el 10 de Octubre de 2020]. Disponible en: http://www.scielo.org.co/pdf/rgps/v10n21/v10n21a06.pdf

1. Se realizó inspección visual de los equipos de cómputo, cableado y verificación de controles de acceso a los centros de cómputo.
2. Se realizó encuesta al administrador de infraestructura y redes, con el fin de conocer las condiciones actuales en materia de seguridad de la entidad.
3. Se consulta la documentación referente a procesos de políticas de seguridad de la información, formalizada, aprobada por el área de calidad y publicada en el portal interno de la institución, con el fin de conocer si se llevan al pie de la letra.

6 DESARROLLO DE LAS FASES

6.1 DESARROLLO FASE 1

- Evaluar de acuerdo con su criticidad, los principales riesgos de seguridad de la información que afrontan las entidades que pertenecen a la red de prestación de servicios de salud en el distrito capital.

  Un fallo de seguridad genera un impacto que puede afectar un activo de información, es por esto que se realiza la probabilidad de ocurrencia en relación a las vulnerabilidades y riesgos, se analizan las consecuencias potenciales de acuerdo a su gravedad la cual puede ser desde dispersión de información hasta robo de información confidencial.[9]

  Los riesgos se clasifican de acuerdo a sus consecuencias potenciales.

[9] ISOTOOLS, 2019, Análisis y evaluación de riesgos de seguridad de la información: identificación de amenazas, consecuencias y criticidad. (2021). Consultado el 23 Enero 2021, Disponible en: https://www.isotools.org/2019/10/18/analisis-y-evaluacion-de-riesgos-de-seguridad-de-la-informacion-identificacion-de-amenazas-consecuencias-y-criticidad/

1- Riesgo Aceptable
2- Riesgo residual

Riesgo Aceptable: En la mayoría de los casos no es posible eliminarlo, ante ello la única opción es reducirlo, tanto en su posibilidad de ocurrencia, como en las consecuencias que puedan afectar los diferentes niveles de la entidad. Este riesgo no debe generar perjuicio que afecte la continuidad del negocio.

Riesgo Residual: Este riesgo permanece a pesar de que se implementen los controles, y/o procesos de mitigación.

La evaluación del riesgo enfocado en la identificación de acuerdo al análisis realizado genera una valoración que determina el grado de riesgo y amenaza potencial asociada.

La identificación de riesgos, amenazas y vulnerabilidades, determinan la clasificación de acuerdo a su criticidad:

- ✓ Alto: Cuando se hace imperativo realizar medidas correctivas, debido a la posibilidad de falla de continuidad en uno o varios sistemas.

- ✓ Medio: Se debe realizar un plan de acciones correctivas en un periodo limitado de tiempo

- ✓ Bajo: De acuerdo al análisis se determina si se hace necesario realizar acciones correctivas.

Riesgos detectados en entidades de salud que hacen parte de la red de prestación de servicios de salud en el distrito capital, de acuerdo a como se indica en el cuadro 1

Cuadro 1. Evaluación de Riesgo

Identificación del riesgo encontrado y su correspondiente calificación, el cual determina la criticidad, ya sea Bajo, Medio o Alto

Riesgo Físico

Recopilación de Información	Clasificación de Riesgo
Centros de Computo (Gabinetes Rack), que en su mayoría no se encuentran cerrados con llave.	Alto
Puntos de red habilitados sin equipo de cómputo conectado	Medio
Puntos de red sueltos a la vista de los usuarios, Jack RJ45 con los cables a la vista.	Bajo
Elementos de conectividad como Switches y Access Point, ubicados en mesas o piso, el cual se encuentra ante manipulación o desconexión por parte del usuario.	Alto
Falla eléctrica, algunas UPS no funcionan	Alto
Inclusión de cableado eléctrico y de red en la misma canaleta sin aislamiento	Medio
Obsolescencia tecnológica, equipos muy antiguos encargados de transmisión de datos aun en funcionamiento.	Alto

Control de Acceso

Recopilación de Información	Clasificación de Riesgo
A pesar de que existe documentación sobre el control de acceso, no se encuentra implementado para los diferentes centros de Computo	Alto

Cuadro 2. Evaluación de Riesgo (Continuación)

Recopilación de Información	Clasificación de Riesgo

El control de acceso a la red para equipos de cómputo personales no se encuentra implementado en todas las sedes de las instituciones, por falta de dispositivos que permitan realizar este control	Alto
Puntos de red que se encuentran habilitados, permiten la conexión de un equipo personal(Usuario Externo), el cual obtiene acceso a las carpetas compartidas de la organización y acceso a internet	Alto
En áreas asistenciales hay equipos de cómputo (portátiles) que se encuentran mesas o centrales de enfermería, que pueden ser objeto de robo.	Alto

Riesgo Lógico

Recopilación de Información	**Clasificación de Riesgo**
No se realiza Backup de la información de manera automatizada a datos de usuarios finales.	Alto
No existen controles de fuga de información	Alto
En la red existen carpetas compartidas con información de historias clínicas, sin implementar control de acceso.	Alto
En algunas sedes no se cuenta con control de acceso a la red inalámbrica, con el solo hecho de conocer la clave permite acceder a la red.	Medio
Equipos de cómputo con sistema operativo sin actualización o parches de seguridad	Medio
La mayoría de equipos asistenciales no cuentan con contraseña de acceso, o la contraseña es publica	Alto
Aunque se cuenta con dominio de red, no se encuentra implementado en todas las sedes, impidiendo el control efectivo de todos los equipos de computo	Alto
Algunas aplicaciones como Suite Ofimática, antivirus o sistemas operativos no cuentan con licenciamiento	Alto
Algunos equipos de uso exclusivo de usuario final, cuentan con servicio web(http - https), publicación de un servicio web	Medio
Algunos usuarios no hacen uso del correo corporativo, utilizan clientes de correo externo como lo son Gmail, Hotmail, Yahoo, etc, para el envió de información institucional	Alto

Cuadro 3. Evaluación de Riesgo (Continuación)

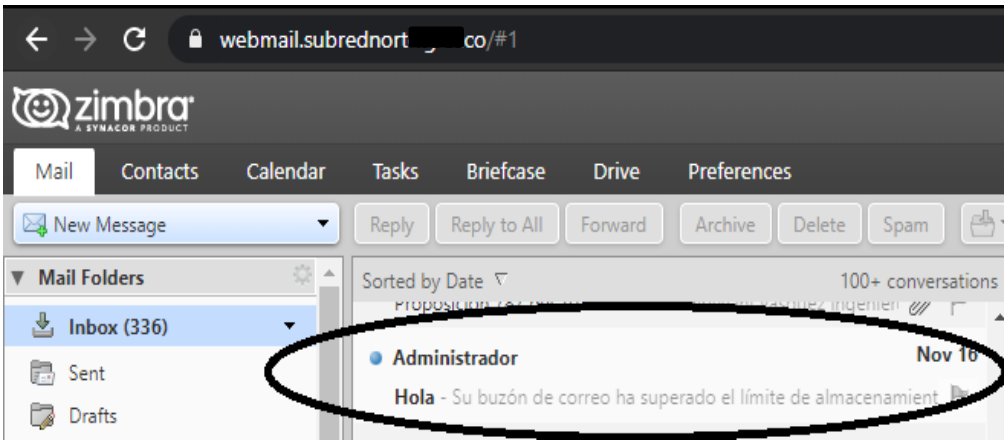
Recopilación de Información	**Clasificación de Riesgo**

Se cuenta con información oficial publicada en herramientas como Google Drive, no se utilizan herramientas propias o no existen.	Alto
Algunos equipos de cómputo no cuentan con Antivirus instalado	Alto

Resumen de Identificación de riesgos y levantamiento de información, en una institución prestadora de servicios de salud del distrito capital. El cual se llevó a cabo en las instalaciones físicas de una entidad de salud, donde se pudo verificar en una cuenta de usuario de correo corporativo, lo siguiente:

1. En la figura 3, se evidencia Spam en Correo Institucional.

Figura 3. Spam Correo Institucional

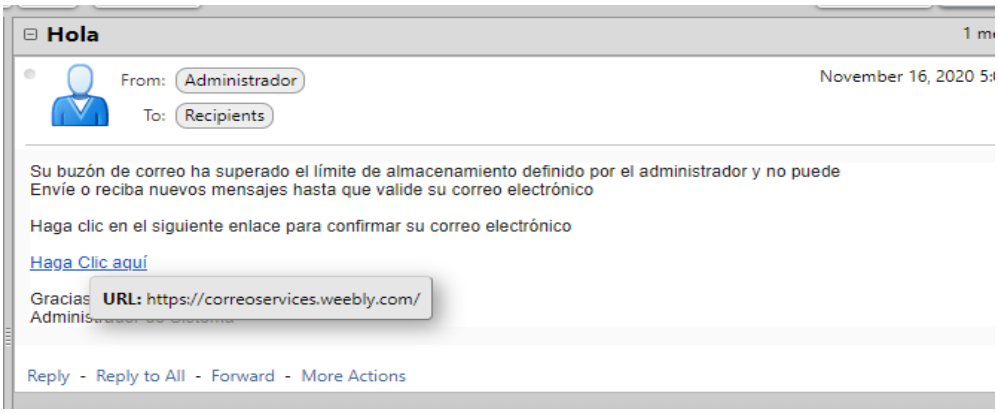


Fuente: El Autor

Se indica que se ha superado el límite de almacenamiento, Su contenido es falso.

Al realizar la verificación del contenido del correo electrónico se identifica que este contenido es falso, de acuerdo a como se evidencia en la Figura 4.

Figura 4. Contenido Falso en Correo Institucional



Fuente: El Autor

- Al realizar identificación visual, se evidencia que uno de los problemas más grandes de seguridad radica en la falta de equipos de cómputo para el personal asistencial, teniendo en cuenta que en los stands de enfermería aproximadamente para 10 profesionales solo cuentan con 4 equipos en promedio. Esto implica que el funcionario al no tener disponibilidad de equipos de cómputo en su lugar de trabajo, acude a traer su equipo personal a la entidad, para el cual se evidencia falta de controles de registro y verificación por pate del área de TIC.

- Se realiza consulta de documentación normalizada y avalada por el área de Calidad frente a Seguridad de la información, publicada en el portal institucional.

1. Documento: Registro de Activos de Información (AP-GI-O-03-03). Aquí se registran los responsables de la información, tipo y custodia de la misma.

2. Documento: Procedimiento Entrada y Salida de Información. Contiene el flujo de proceso desde la solicitud del dato hasta su publicación o entrega.

3. Documento: Plan de Tratamiento del Riesgo de la Información (AP-GI-PL-03-02): Aquí se plasman las actividades asociadas al plan de tratamiento, enfocado en el autodiagnóstico, alcance, identificación, definición y análisis del riesgo.

4. Documento: Plan de Comunicación y Divulgación del Modelo de Seguridad y Privacidad de la Información (AP-GI-PL-09-01): Busca generar una cultura de seguridad de la información a los empleados de la institución con el fin de presentar el modelo de optimización en el flujo de información de la entidad.

5. Documento: Plan de Contingencia de los Sistemas de Información: Se enfoca en generar ruta crítica con el fin de promover el uso de recursos informáticos.

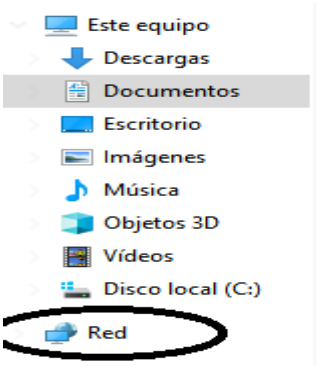
- Dentro de la información consultada, no se encuentra un protocolo de acceso a equipos de cómputo de terceros, es decir que un funcionario que solicite permisos de acceder a la red, es permitido, pero no se realiza verificación de legalidad de software, actualizaciones al sistema operativo, estado de antivirus, etc

- Aunque se cuenta con un dispositivo Firewall (Fortinet 1000D), no se implementa el módulo de Prevención de intrusiones - IPS y Prevención de perdida de datos - DLP

- Se realiza la tarea de conectar un equipo personal a un punto de red en una sede prestadora de servicios de salud, el cual permite acceder a la red. Esto quiere decir que no existe un control de acceso a dispositivos personales en esta sede.

En un proceso básico que puede realizar cualquier usuario, se accede a las carpetas del computador conectado a la red, de acuerdo a como se visualiza en la figura 5.

Figura 5. Ruta Acceso red Institucional

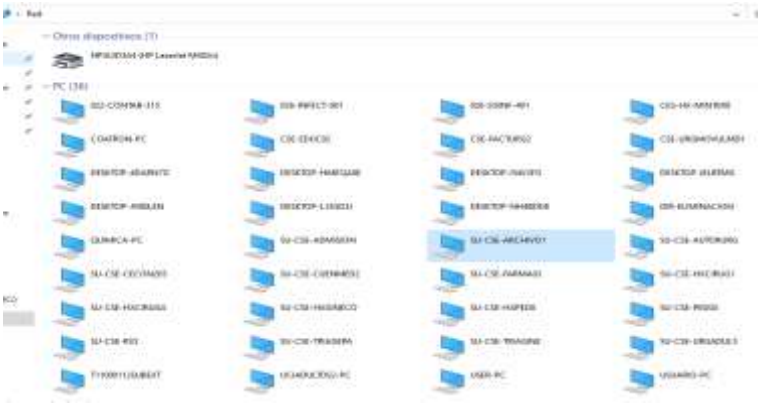


Fuente: *El Autor*

Se procede a ingresar a consultar la red, en busca de equipos que se encuentran conectados y comparten un recurso (Carpetas, Impresoras, etc).

De acuerdo a la Figura 6, al ingresar se genera el siguiente listado:

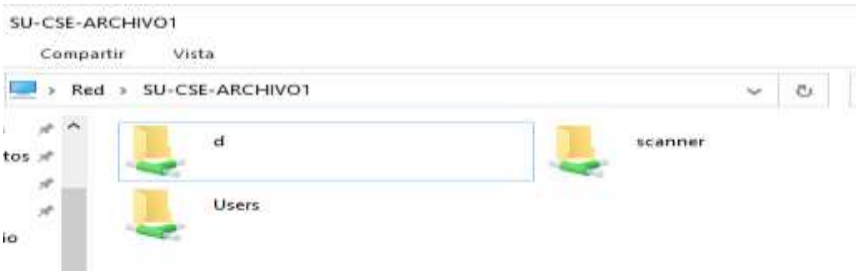
Figura 6. Acceso a la red Institucional Usuario Final



Fuente: *El Autor*

Según la Figura 7, se selecciona un equipo de manera aleatoria: (SU-CSE-ARCHIVO1).

Figura 7. Acceso a Carpetas Compartidas equipo en Red

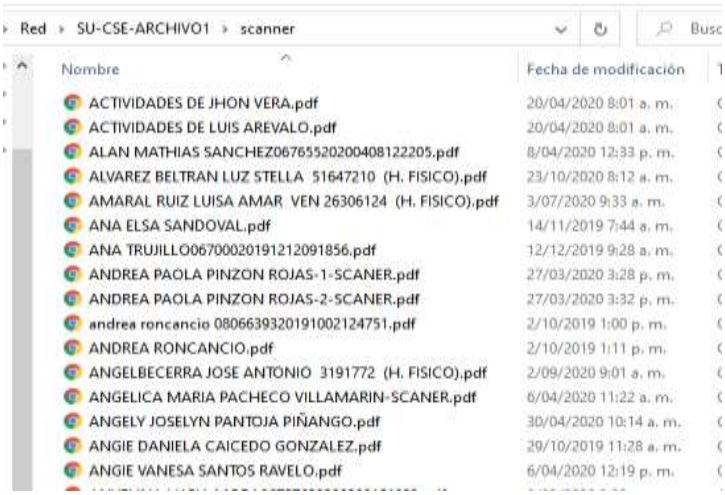


Fuente: *El Autor*

Donde se puede evidenciar que cuenta con carpetas compartidas (Esto implica riesgo a la información).

Al continuar realizando consultas, se evidencia de acuerdo a la Figura 8, que los usuarios tienen el permiso de compartir carpetas, donde publican cualquier tipo de información.

Figura 8. Acceso a Información Compartida Institucional



Fuente: *El Autor*

Al realizar la revisión de uno de estos archivos se evidencia que son historias clínicas de pacientes, que puede fácilmente cualquier persona acceder a ellas.

Se realiza inspección visual de las condiciones de infraestructura.

- En la Figura 9, se identifican puntos de red que se encuentran sueltos o en malas condiciones, en puestos de trabajo

Figura 9. Puntos de red deteriorados o sueltos

Fuente: *El Autor*

- Se evidencia que algunos equipos no solicitan clave de acceso, o en algunos equipos es el mismo usuario y la misma contraseña (Usuario y contraseña genérico)

6.2 DESARROLLO FASE 2

- Justificar la necesidad de implementar acciones, procesos y procedimientos, enfocados a la seguridad de la información.

Dentro de las entidades del sector salud se hace necesario implementar todos los mecanismos que apoyen el ejercicio de análisis, documentación y toma de decisiones frente a la mitigación del riesgo, con el fin de evitar fugas de información, Teniendo en cuenta que la información contenida es de carácter confidencial y se encuentra protegida mediante normas establecidas por el gobierno. Es por ello la importancia de hacer énfasis no solo en la prestación del servicio, sino en garantizar el correcto almacenamiento y respaldo de la información.

El sistema informático en cualquier entidad, para ser considerado seguro, debe en primer lugar ser accesible solo a personal autorizado y contar con alta disponibilidad. El uso malicioso de los sistemas de información y de todos aquellos recursos internos, puede acarrear consecuencias desastrosas afectando directamente la productividad.

La entidad almacena información sensible, de reserva legal, como lo son las historias clínicas tanto digitales como en físico, es por ello que se deben implementar todos los procesos, procedimientos y controles necesarios para proteger la información.

Hacer uso de controles de Acceso, definir políticas de seguridad de la información y responsabilizar al personal en el acatamiento de las mismas, así como realizar los controles de mitigación de riesgos y vulnerabilidades, permitirá un uso confiable de las herramientas de información y un soporte técnico menos desgastante.

Los modelos principales de control de acceso hacen referencia a un conjunto de criterios que definen derechos, permisos de un usuario a un sistema.

a. Control de Acceso Obligatorio (Mandatory Acces Control - MAC): Control de acceso de usuarios a recursos basados en derechos establecidos por una autoridad.
b. Control de Acceso Discrecional (Discretionary Acces Control - DAC): Control de acceso a objetos basados en la identidad de los sujetos y/o grupos que pertenecen.
c. Control de Acceso Basado en Roles (Rule Based Acces Control - RBAC): Control de acceso basado en permisos o roles, asigna funciones y privilegios a usuarios. Los archivos y recursos se asignan a permisos de acuerdo a las funciones necesarias.

La implementación de modelos de seguridad de la información no genera ingresos a las entidades, sin embargo, reduce costos de reparación de los incidentes generados.

La norma ISO 27001 indica los 4 principales beneficios en la implementación de Sistemas de seguridad de la información[10].

1. Cumplimiento: Relacionado a los aspectos generales de garantizar la seguridad protección, privacidad y seguridad de los datos.
2. Ventaja Competitiva: Teniendo en cuenta que las entidades del sector salud manejan información altamente sensible, se hace necesario garantizar la disponibilidad y seguridad que permita gestión oportuna.
3. Disminución de gastos ante incidentes: Entre menos incidentes de seguridad menos es el gasto de solución a los mismos.
4. Organización: la asignación de roles implica responsabilidades, que deben ser definidas para garantizar un buen desempeño en función de producción de la entidad.

[10] ISOTOOLS, 2019, BENEFICIOS DE IMPLEMENTAR UN SG DE SEGURIDAD DE LA INFORMACIÓN, [CONSULTADO EL 1 DE MARZO DE 2021].,, DISPONIBLE EN: HTTPS://WWW.ISOTOOLS.ORG/2019/01/11/5-BENEFICIOS-IMPLEMENTAR-SISTEMA-GESTION-SEGURIDAD-INFORMACION/

6.3 DESARROLLO FASE 3

- Recomendar al personal encargado de TIC, de acuerdo con el análisis realizado, los procedimientos y mecanismos que permitan la mitigación de riesgos y vulnerabilidades.

A continuación, se realizan las siguientes recomendaciones con respecto a procedimientos y políticas, que de acuerdo al análisis podrían ser implementadas.

1. Recomendación de Procedimiento de control de Acceso a equipos de cómputo:

   Todo dispositivo que requiera acceso a la red institucional debe ajustarse al siguiente procedimiento:

   1.1 Solicitud por parte del líder de Proceso (Jefe inmediato del funcionario), justificando la necesidad de conectar este equipo a la red, indicando marca y serial del dispositivo.

   1.2 Recepción de la solicitud por parte del personal encargado. (Aquí se gestiona la viabilidad de la solicitud).

   - Si existen equipos en stock para entrega, se rechaza solicitud y se asigna equipo institucional al servicio o funcionario.

   - Si la finalidad de la conexión es para fines diferentes a funciones relacionadas con el cargo, la solicitud se rechaza.

   - Si la infraestructura tecnológica (Switches, Access Point, Switch Core, etc), no permiten la inclusión de más equipos, la solicitud se rechaza.

- Si la infraestructura física (Equipos de escritorio, Stand de Enfermería, oficinas, etc.), no se encuentran disponibles para ubicar el equipo de cómputo, la solicitud se rechaza.

1.3 Realizar verificación al equipo de cómputo, para permitir o no, acceso a la red.

- Verificar que la Marca y Serie del dispositivo corresponde al solicitado por parte del líder de proceso.

- Realizar verificación de legalidad de software instalado. La solicitud se rechaza en dado caso de que el equipo no cuente con software legal.

- Realizar verificación de parches de seguridad para el software instalado.

- Realizar verificación de Software Antivirus (Legalidad, versión de actualización de firmas).

- Realizar revisión de software instalado, con el fin de verificar que no se encuentre software que pueda generar tráfico en la red.

1.4 Se procede a realizar el registro en red, mediante la dirección física MAC Address, el cual permitirá realizar seguimiento del dispositivo.

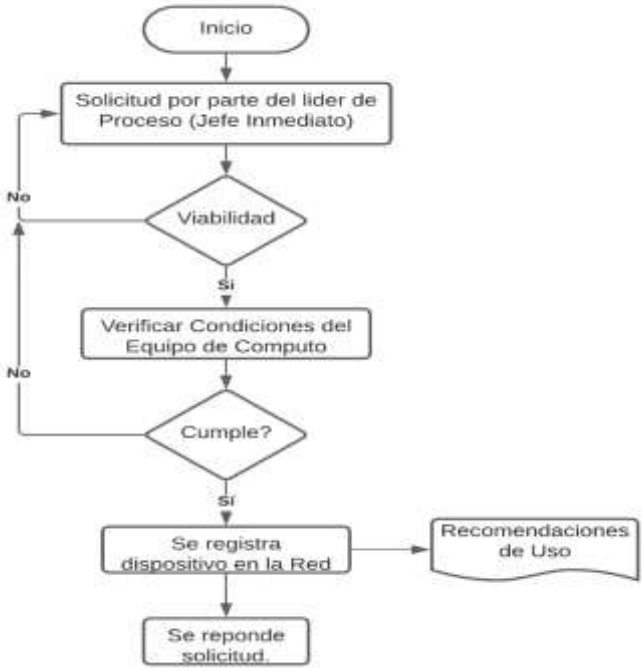
1.5 Incluir el dispositivo en las reglas de uso básico del firewall, dependiendo de las funciones a realizar, se crearán las excepciones necesarias.

1.6 Realizar las recomendaciones correspondientes al buen uso de la red e información institucional que pueda derivar de esta.

1.7 Responder la solicitud al líder de proceso, indicando el resultado de la misma.

En la Figura 10, Se expresa el Diagrama (Procedimiento control de Acceso).

Figura 10: Diagrama de flujo – Control de acceso



Fuente: *El Autor*, publicado en: https://lucid.app/lucidchart/invitations/accept/90851081-cc00-47fe-8860-16a3b2c33ff0

2. Recomendación de políticas de Seguridad.

Con el fin de minimizar los riesgos, se proponen las siguientes políticas de seguridad de la información.

- Políticas de transferencia de información:

  - La información institucional que requiera ser trasladada ya sea entre sedes de la empresa o al exterior de la misma, se realizara mediante los dispositivos móviles asignados al funcionario, los cuales utilizaran herramientas de cifrado de datos para la protección de la información, apoyado bajo los procedimientos de salida de dispositivos.

  - Los propietarios de los activos de información que requieran trasladar información en dispositivos externos (USB, CD, DVD), son responsables de evitar divulgación no autorizada y deben garantizar la confidencialidad de la información, deberán adoptar una cultura de seguridad de la información la cual se encontrara sustentada dentro de los procesos de seguridad que se encuentren definidos y aprobados

Políticas de Uso de Correo corporativo.

  - Capacitar al personal que hace uso de la plataforma de correo corporativo, para que este pueda identificar la legalidad de un correo recibido, con el fin de evitar él envió de información sensible a personal ajeno a la institución.

  - El correo corporativo es de uso exclusivo de los funcionarios de la entidad, es por ello que no se debe permitir acceso a terceros, o hacer uso para envió o recepción de información personal.

Políticas de Control de Acceso.

- El área de TIC's debe implementar los mecanismos, procesos o procedimientos propios para establecer control de acceso sobre los Activos de información de la entidad (Centros de cómputo, servidores, equipos de usuario final, red, etc).

- Los funcionarios de la entidad, no prestaran las claves de acceso a los computadores asignados o a las distintas aplicaciones donde se registre información institucional. Los datos de acceso son unipersonales.

- El administrador de cuentas de usuarios, debe implementar el cierre de sesión automático, por tiempo de tiempo inactividad, en un periodo no superior a 10 minutos.

- Implementar por parte del administrador de Red como parte del control de acceso a la red, el control de contenido Web, limitar las descargas, realizar las excepciones necesarias de acuerdo al perfil y necesidad del cargo.

6.4 DESARROLLO FASE 4

- Diseñar una matriz de vulnerabilidades que apoye la creación de un modelo de políticas de Seguridad.

  Para el desarrollo de este objetivo se proponen las escalas de impacto de acuerdo al riesgo, el cual se expresa en el cuadro 2.

Cuadro 4. Nivel de Impacto

Valoración de Nivel de impacto de acuerdo a Riesgo que representa la información en la entidad

IMPACTO	VALOR
ALTO	3
MEDIO	2
BAJO	1

Dentro del Cuadro 3, se indica la matriz de vulnerabilidades

Cuadro 3. Riesgo, Impacto y Control del Riesgo

Identificación del Riesgo, Impacto que genera a la información y el control que se debe implementar

Ítem	Riesgo	Impacto	Control del Riesgo
1	Control de Accesos deficiente en Racks de Comunicaciones	3	Diseño e implementación de política, que implique el aseguramiento de estos centros de computo
2	Puntos de red habilitados sin equipo de cómputo conectado	2	Realizar la revisión periódica de puntos de red de la institución, con el fin de deshabilitar los que no se encuentren en uso
3	Puntos de red sueltos a la vista de los usuarios, Jack RJ45 con los cables a la vista.	3	Realizar la reparación oportuna de puntos de red que se encuentren en mal estado

Cuadro 3. Riesgo, Impacto y Control del Riesgo (Continuación)

Item	Riesgo	Impacto	Control del Riesgo
5	Inclusión de cableado eléctrico y de red en la misma canaleta sin aislamiento	3	Realizar la distribución correspondiente y adecuada diferenciando el tipo de cableado, con el

			fin de evitar interferencias electromagnéticas
6	Obsolescencia tecnológica, equipos muy antiguos encargados de transmisión de datos aun en funcionamiento.	2	En la medida de lo posible, realizar las actualizaciones al software y realizar los cambios de manera gradual a medida que el presupuesto lo permita.

7 CONCLUSIONES

Teniendo en cuenta la criticidad en los riesgos de seguridad, un problema evidente, corresponde al deficiente control de acceso de dispositivos personales, se podría asumir que una persona que por algún motivo conecta su equipo a la red a pesar de que el administrador lo permita por medio de control de acceso, este equipo posiblemente pueda contener un virus y generar una contaminación a todos los dispositivos de la red, o que este usuario descargue información correspondiente a Historias clínicas, a las cuales les pueda dar un uso indebido, o peor aún, que este usuario cuente con los conocimientos suficientes para realizar procesos de captura de información en la red, denegación de servicio (DDos), spoofing, etc.

Se evidencia que los riesgos asociados a seguridad de la información en primer lugar se determinan por la falta de controles efectivos, ya que a pesar de que existe documentación, no se implementan procesos y procedimientos que permitan la mitigación del riesgo, además se evidencia que no hay personal directamente encargado de la seguridad de la información, más bien cada funcionario se encarga de proteger a su manera y hacer controles de acuerdo a su criterio, mas no siguiendo las normas documentadas, de esta manera se justifica la necesidad de integrar las acciones, procesos y procedimientos que permitan una gestión unificada a la seguridad de la información en estas entidades.

De acuerdo a la encuesta realizada, se evidencia que el personal es consciente de las faltas de controles existentes, las cuales exponen de manera significativa la seguridad de los activos de información, no existe un control apropiado de registro de equipos de cómputo de terceros. Es por ello que se hace necesario hacer énfasis en las recomendaciones descritas, para abordar y solucionar a las dificultades encontradas.

Teniendo en cuenta el resultado de la matriz de vulnerabilidades se evidencia que, aunque se encuentra documentación referente a políticas de seguridad de la información, estas no se implementan, se identifica, la necesidad urgente de enfocarse en implementar por los menos los controles documentados y tomar en cuenta las observaciones presentadas, con el fin de mitigar el riesgo.

8 RECOMENDACIONES

Luego del resultado obtenido del análisis de las vulnerabilidades en la entidad, se realizan las siguientes recomendaciones.

- No responder correos que soliciten información de salud de los pacientes.
- Capacitar al personal, para que tome la precaución necesaria al descargar archivos adjuntos de correos electrónicos.
- No utilizar cuentas de correo corporativos para envió de información personal.
- No compartir contraseñas, ni solicitar las de otro funcionario.
- No abrir correos donde el asunto indica que se debe cambiar la contraseña o que indique que el buzón se ha llenado.
- El área de Soporte técnico de TIC, debe garantizar el escaneo inmediato por medio de un antivirus, al introducir dispositivos USB en los equipos de cómputo.
- Evitar por parte de todos los funcionarios, guardar información en el área de Escritorio(Desktop), del equipo de cómputo.
- Controlar el software instalado en cada equipo de cómputo de acuerdo a las funciones relacionadas al usuario.
- Todo equipo de cómputo personal de un tercero (Personal asistencial), debe contener software licenciado, debe encontrarse actualizado. Contar con antivirus y su uso debe autorizarlo el lidero de proceso. El registro del equipo se realizará en la red mediante la dirección física MAC Address.
- Se debe realizar ajustes de organización, actualización de etiquetado al cableado, en los centros de cómputo, y ajuste en tomas RJ45 en puestos de trabajo que se encuentran sueltas, expuestas a condiciones de humedad o manipulación indebida por parte de los usuarios.
- Se debe unificar el nombre de la red inalámbrica, ya que en algunos pisos o sedes la red tiene diferentes nombres que no hacen referencia institucional.

- Se debe priorizar el uso de la plataforma de correo corporativo, impedir el acceso a cuentas de correo personal para el envió de información institucional.

BIBLIOGRAFÍA

ALCALDIA MAYOR DE BOGOTA, DISTRITO CAPITAL. Acuerdo 641 de 2016. {En línea}. [Consultado el 20 de Octubre de 2020]. Disponible en: http://www.saludcapital.gov.co/Inst_Coordinacion/CDSSS/Normativa/Relacionado_Acuerdo_641_2016.pdf

BARRIENTOS, Juan. La evaluación de nuevas tecnologías en salud en hospitales. {En línea}. (2016). [Consultado el 10 de Septiembre de 2020]. Disponible en: https://www.redalyc.org/pdf/1590/159049704006.pdf

BERNAL, Forero. Sistemas de información en el sector salud en Colombia. {En línea}. (2011). [Consultado el 20 de Octubre de 2020]. Disponible en: http://www.scielo.org.co/pdf/rgps/v10n21/v10n21a06.pdf

BERNAL, Forero. Sistemas De Información En El Sector Salud En Colombia. [online] Scielo.org.co {En línea}. (2011). [Consultado el 30 de Noviembre de 2020]. Disponible en: <http://www.scielo.org.co/pdf/rgps/v10n21/v10n21a06.pdf>

CAMARA DE COMERCIO DE BOGOTA D.C. Ciberseguridad, tendencias y retos en salud electrónica: tópicos de HIMSS Colombia 2017. {En línea}. [Consultado el 10 de Septiembre de 2020]. Disponible en: https://www.ccb.org.co/Clusters/Cluster-de-Salud-de-

CABALLERO, Gogler. Centro de Informática en Salud: una propuesta actual. {En línea}. (2011) [Consultado el 28 de Octubre de 2020]. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592011000200008

CARRILLO, Juan. Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. {En línea}. (2014). [Consultado el 9 de Septiembre de 2020]. Disponible en: https://www.sciencedirect.com/science/article/pii/S0212656714000067

CUERVO. José. INFORMATICA JURIDICA. {En línea}. 2018 [Consultado el 7 de Marzo de 2021]., Disponible en: http://www.informatica-juridica.com/author/josecuervo/

DIAZ, Ricardo. Sistema Para al Gestion de la Informacion en la Universidad de Ciencias Medicas de HOLGUIN. {En línea}. (2014). [Consultado el 10 de Septiembre de 2020]. Disponible en: https://www.redalyc.org/pdf/1815/181531232002.pdf

Español, I. (2019). Iso 27002 Español [k5466rgmp948]. {En línea}. [Consultado el 7 de Marzo de 2021]., Disponible en: https://idoc.pub/documents/iso-27002-espaol-k5466rgmp948

FERNANDEZ, J., CARRION, I., OLIVER, P., & TOVAL, A. (2013). Seguridad y privacidad en las historias clínicas electrónicas: una revisión sistemática de la literatura. {En línea}. [Consultado el 9 de Septiembre de 2020]. Disponible en: https://www.sciencedirect.com/science/article/pii/S1532046412001864

GARCIA, ROCHIN, RAMON (2007). ¿Qué es la informática de la salud? Salud en Tabasco, 13(1),607-610. {En línea}. [fecha de Consulta 9 de Septiembre de 2020]. ISSN: 1405-2091. Disponible en: en: https://www.redalyc.org/articulo.oa?id=487/48713109

GLOSARIO – Secretaría Distrital de Salud. (2017). {En línea}. [Consultado el 7 de Marzo de 2021]., from http://www.saludcapital.gov.co/Documents/Transparencia/Glosario.pdf

GLOSARIO DE CIBERSEGURIDAD. (2021). {En línea}. [Consultado el 7 de Marzo de 2021]., Disponible en: https://www.agilescrum.cl/post/glosario-de-ciberseguridad

GUÍA DE AJUSTE DEL SISTEMA INTEGRADO DE GESTIÓN DISTRITAL. (2021). {En línea}. [Consultado el 7 de Marzo de 2021]., from https://secretariageneral.gov.co/sites/default/files/tomoiiguiadeajustesver.pdf

Guía Técnica Para La Gestión Del Riesgo de Desastres en El Contexto Hospitalario (GRDCH). (2017). [Consultado el 7 de Marzo de 2021]., {En línea}. Disponible en: https://es.scribd.com/document/429925082/Guia-Tecnica-Para-La-Gestion-Del-Riesgo-de-Desastres-en-El-Contexto-Hospitalario-GRDCH

GUILLEN, E., RAMIREZ, L., & ESTUPIÑAN, E. (2011). Vista de Análisis de seguridad para el manejo de la información médica en telemedicina | Ciencia e Ingeniería Neogranadina. {En línea}. [Consultado el 9 de Septiembre de 2020]. Disponible en: https://revistas.unimilitar.edu.co/index.php/rcin/article/view/260/1899

INCIBE, I., 2020. GLOSARIO DE TERMINOS DE CIBERSEGURIDAD. [online] Incibe.es. {En línea}. [Consultado el 30 de Noviembre de 2020], Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

ISOTOOLS. ¿En qué consiste el ciclo PHVA de mejora continua?. (2020). {En línea}. [Consultado el 10 de Septiembre de 2020]. Disponible en: https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/

ISOTOOLS, 2019, Análisis y evaluación de riesgos de seguridad de la información: identificación de amenazas, consecuencias y criticidad. (2021). {En línea}. [Consultado el 23 de Enero de 2020]., Disponible en: https://www.isotools.org/2019/10/18/analisis-y-evaluacion-de-riesgos-de-

seguridad-de-la-informacion-identificacion-de-amenazas-consecuencias-y-criticidad/

JOYA, Javier. Avesalud IPS, Desarrollo de una Propuesta de Mitigación de Riesgos y Vulnerabilidades en Activos Lógicos para la Empresa Javesalud I.P.S. {En línea}. [Consultado el 28 de Octubre de 2020]. Disponible en: https://repository.ucatolica.edu.co/bitstream /10983/15405/1/Proyecto%20Final%20Especializacion%20Seguridad%20de%20la %20Informacion.pdf

GONZALEZ, Bernaldo de Quiros, F. (2015). Sistemas de Información en Salud: Integrando datos clínicos en diferentes escenarios y usuarios. {En línea}. [Consultado el 28 de Octubre de 2020]. Disponible en: http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1726-46342015000200020

MOJERON, Giraldoni. Problemas éticos y de seguridad asociados al uso de las tecnologías de la información y el conocimiento en Salud. {En línea}. (2008). [Consultado el 10 de Septiembre de 2020]. Disponible en: https://www.redalyc.org/pdf/1800/180020294017.pdf

MINISTERIO DE LAS TELECOMUNICACIONES – MINTIC. {En línea}. [Consultado el 20 de Octubre de 2020]. 2020 Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MINISTERIO DE LAS TELECOMUNICACIONES – MINTIC. {En línea}. [Consultado el 21 de Octubre de 2020]. 2010 Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MINISTERIO DE SALUD. Relación de Conjunto de Datos por temáticas - Datos Abiertos (datos.gov.co). {En línea}. 2020 [Consultado el 20 de Octubre de 2020]. Disponible en: https://www.minsalud.gov.co/Paginas/datos-abiertos.aspx

MINISTERIO DE TECNOLOGIAS DE INFORMACION Y TELECOMINICACIONES – MINTIC. Normograma del Ministerio de Tecnologías de la Información y las Comunicaciones [DECRETO_0780_2016]. (2021). {En línea}. [Consultado el 7 de marzo de 2021]., Disponible en: https://normograma.mintic.gov.co/mintic/docs/decreto_0780_2016.htm

PLAZZOTTA, Fernando. Sistemas de Información en Salud, {En línea}.(2015). [Consultado el 10 de septiembre de 2020]. Disponible en: https://www.redalyc.org/pdf/363/36341083020.pdf

INSTITUTO NACIONAL DE SALUD, Plan de Seguridad y Privacidad en la Información. (2018). {En línea}. [Consultado el 21 de Octubre de 2020]. Disponible en: https://www.ins.gov.co/Transparencia/Planesestratgicossectorialesinstitucionales/PLANDESEGURIDADYPRIVACIDADDELAINFORMACIONINS.pdf

GONZALEZ Bernaldo de Quiroz, F. (2020). Sistemas de Información en Salud: Integrando datos clínicos en diferentes escenarios y usuarios. {En línea}. [Consultado el 21 de Octubre de 2020]. Disponible en: https://www.scielosp.org/article/rpmesp/2015.v32n2/343-351/

SECRETARIA DISTRITAL DE SALUD. Política de Seguridad de la información de la SDS {En línea}. (2012). [Consultado el 21 de Octubre de 2020]. Disponible en: http://190.25.230.149/Polticas%20en%20Formulacin/POLITICA%20DE%20SEGURIDAD%20DE%20LA%20INFORMACION.pdf

PRADOS, José. (2012). Telemedicine, also a tool for the Family Doctor. {En línea}. [Consultado el 10 de Septiembre de 2020]., Disponible en: https://core.ac.uk/download/pdf/82680868.pdf

RUIZ, Luis. (2014). Diseño de Modelo de Seguridad Informática. {En línea}. [Consultado el 9 de Septiembre de 2020]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2976/Trabajo%20de%20grado1518.pdf?sequence=1

LATERRA, Cristina. La Informática en los Hospitales. {En línea}. (2001). [Consultado el 10 de Septiembre de 2020]. Disponible en: https://www.redalyc.org/pdf/912/91220101.pdf

SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ES.E., Código de Ética y Buen Gobierno. (2021). {En línea}. [Consultado el 7 de Marzo de 2021]., Disponible en: https://www.subrednorte.gov.co/intranet/images/Subred%20Norte/Codigo%20de%20etica%20y%20buen%20gobierno.pdf

SECRETARIA SENADO. Ley 527 de 1999. {En línea}. 2020 [Consultado el 30 noviembre de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

URREGO, Hernando, ESTÁNDAR GERENCIA DE LA INFORMACION. (2018). {En línea}. [Consultado el 21 de Octubre de 2020]. Disponible en: https://ese-hospital-de-aguazul-juan-hernando-urrego.micolombiadigital.gov.co/sites/ese-hospital-de-aguazul-juan-hernando-urrego/content/files/000147/7339_plan-de-seguridad-y-privacidad-de-la-informacion.pdf

VEGA, Walter. Políticas y Seguridad de la Información. {En línea}. (2008). [Consultado el 28 de Octubre de 2020]. Disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008#:~:text=Las%20pol%C3%ADticas%20de%20seguridad%20se,y%20disponibilidad%20de%20la%20informaci%C3%B3n.

VALDERRAMA, Jhon. Pentesting “Prueba de Penetración” Para la Identificación de vulnerabilidades en la red de computadoras en la Alcaldía del Municipio de Canton del San Pablo, Departamento de Choco. {En línea}. (2017). [Consultado el 28 de Octubre de 2020]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/18049/1077436201.pdf?sequence=1&isAllowed=y

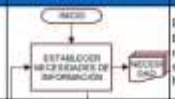
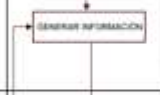
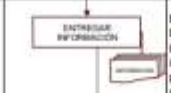
VALENZUELA, José. (2016). Fundamentos de la informática en salud. {En línea}. [Consultado el 10 de Septiembre de 2020]. Disponible en: https://www.redalyc.org/pdf/1631/163147636011.pdf

VIDAL, Maria. Información, informática y estadísticas de salud: un perfil de la tecnología de la salud. {En línea}. (2004). [Consultado el 28 de Octubre de 2020]. Disponible en: http://scielo.sld.cu/scielo.php?pid=S1024-94352004000400008&script=sci_arttext&tlng=pt

VIDAL, Maria. Revista Cubana de Informática Médica (RCIM). {En línea}. (2020). [Consultado el 9 de Septiembre de 2020]. Disponible en: http://www.rcim.sld.cu/revista_7/articulo_htm/segurinfsalud.htm

ANEXOS

Anexo A: Procedimiento salida y entrega de información

DESCRIPCIÓN DEL PROCEDIMIENTO						
PHVA	ACTIVIDAD (Flujo grama)	DESCRIPCIÓN (Como)	RESPONSABLE	TIEMPO	DOCUMENTO Y/O REGISTRO GENERADO	PUNTO DE CONTROL (Barreras de Seguridad)
P		ESTABLECER NECESIDADES DE INFORMACIÓN Establecer qué necesidades de información está requiriendo cada uno de los procesos y subprocesos, usando la Matriz Detección Necesidades de Información	Área o Proceso y subproceso que Solicita el Requerimiento	Cada vez que se requiera	Matriz Detección Necesidades de Información	Matriz avalada y firmada por referente del proceso
P		SOLICITUD PROCEDENTE? Evaluar el alcance del requerimiento junto con el usuario del proceso y subproceso o área solicitante.	Ingeniero Soporte de Sistema o del Sistema de Información - Coordinador del Área o Proceso	Cada vez que se requiera	Mesa de Servicios, correo electrónico, oficios internos y externos	Verificación de solicitud
H		GENERAR LA INFORMACIÓN Realizar la actividad correspondiente ya sea por medio de un query, reporte, desarrollo paralelo al Sistema de Información u otro aplicativo activo de la institución, o adquisición de herramienta. También se tienen en cuenta fuentes de origen manual que complementan la información	Ingeniero Soporte de Sistema o del Sistema de Información - Coordinador del Área o Proceso	Cada vez que se requiera	Reporte, consulta, minería de datos	
V		Verificar la información generada, se unifica si es el caso, se evalúa y se valida si es el caso. Para ello se debe implementar el procedimiento de Transformación y verificación de los datos.	Ingeniero Soporte de Sistema o del Sistema de Información - Coordinador del Área o Proceso	Cada vez que se requiera	Reporte, consulta, minería de datos	Validación del reporte cumple con la solicitud
A		ENTREGAR INFORMACIÓN Entregar en medio magnético si es el caso, o a través del recurso de red, correo electrónico, Chat interno, al proceso y subproceso o área solicitante para su análisis y posterior envió a los entes de control tanto internos como Externos.	Ingeniero Soporte de Sistema o del Sistema de Información - Coordinador del Área o Proceso	Cada vez que se requiera	Reporte, consulta, minería de datos	Entrega formalizada a través de correo, medio físico o mesa de servicios
A		REGISTRAR SOLUCIÓN O RESPUESTA Se registra solución o respuesta y se genera notificación al usuario a través del correo electrónico, invitándolo a realizar la calificación del servicio recibido en los casos que aplica.	Ingeniero Soporte de Sistema o del Sistema de Información - Coordinador del Área o Proceso	Cada vez que se requiera	Respuesta a través de correo electrónico, mesa de servicios o medio magnético o físico.	

Fuente: Portal interno institucional – Subred Integrada de Servicios de Salud E.S.E. Formato: AP-GI-P-02-03

Anexo B: Acuerdo 641 DE 2016

ACUERDO 641 DE 2016

(Abril 06)

Por el cual se efectúa la reorganización del Sector Salud de Bogotá, Distrito Capital, se modifica el Acuerdo 257 de 2006 y se expiden otras disposiciones

EL CONCEJO DE BOGOTÁ, D.C.,

En ejercicio de sus facultades constitucionales y legales, en especial las conferidas por los artículos 313 y 322 de la Constitución Política y los artículos 12 numerales 8, 9 y 10; 55 y 63 del Decreto Ley 1421 de 1993,

ACUERDA:

CAPÍTULO I

DISPOSICIONES GENERALES

ARTÍCULO 1º. Objeto. El presente Acuerdo tiene por objeto efectuar la reorganización del sector salud en el Distrito Capital definiendo las entidades y organismos que lo conforman, para lo cual se determinará la fusión de algunas entidades y la creación de otras.

CAPÍTULO II

FUSIÓN DE ENTIDADES

ARTÍCULO 2º. Fusión de Empresas Sociales del Estado. Fusionar las siguientes Empresas Sociales del Estado, adscritas a la Secretaría Distrital de Salud de Bogotá, D.C., como sigue:

Empresas Sociales del Estado de: Usme, Nazareth, Vista Hermosa, Tunjuelito, Meissen y El Tunal se fusionan en la Empresa Social del Estado denominada "Subred Integrada de Servicios de Salud Sur E.S.E."

Empresas Sociales del Estado de: Pablo VI Bosa, del Sur, Bosa, Fontibón y Occidente de Kennedy se fusionan en la Empresa Social del Estado denominada "Subred Integrada de Servicios de Salud Sur Occidente E.S.E."

Empresas Sociales del Estado de: Usaquén, Chapinero, Suba, Engativá y Simón Bolívar se fusionan en la Empresa Social del Estado denominada “Subred Integrada de Servicios de Salud Norte E.S.E.”

Empresas Sociales del Estado de: Rafael Uribe, San Cristóbal, Centro Oriente, San Blas, La Victoria y Santa Clara se fusionan en la Empresa Social del Estado denominada “Subred Integrada de Servicios de Salud Centro Oriente E.S.E.”

PARÁGRAFO 1. Cada una de las cuatro Empresas Sociales del Estado producto de la fusión prestarán servicios integrales de salud de todos los niveles de complejidad y se articularán en una sola Red Integrada de Servicios de Salud Distrital de conformidad con el artículo 25 del presente Acuerdo.

PARÁGRAFO 2. Los nombres de las actuales unidades de prestación de servicios de salud deberán conservarse para efectos de la identificación por parte de la ciudadanía.

PARÁGRAFO 3. En cada una de las subredes de prestación de servicios de salud se desarrollará una central de urgencias de conformidad con las necesidades de la población, la demanda de servicios y la accesibilidad geográfica.

PARÁGRAFO 4. Las cuatro subredes de servicios de salud adelantarán las acciones de promoción de la salud y prevención de la enfermedad a nivel individual y colectivo que le brinden al usuario una atención integral. Se fortalecerán las acciones de autocuidado y mutuo cuidado y las acciones intersectoriales que fomenten acciones individuales y colectivas para incentivar estilos de vida saludable.

PARÁGRAFO 5. Las Empresas Sociales del Estado resultantes de la fusión deberán realizar, conforme a la normatividad vigente, procesos de rendición de

cuentas ante la comunidad beneficiaria con el fin de promover la participación ciudadana e implementar las acciones que mejoren los servicios de salud.

ARTÍCULO 3º. Transición del proceso de fusión de las ESE. Ver Decreto Distrital 171 de 2016. Con el fin de efectuar la expedición de los actos administrativos, presupuestales y demás trámites necesarios para el perfeccionamiento del proceso de fusión de las Empresas Sociales del Estado, se establece un periodo de transición de un año contado a partir de la expedición del presente Acuerdo.

Durante el periodo de transición se seguirán las siguientes reglas:

a). La dirección y administración de las Empresas Sociales del Estado resultantes de la fusión, durante este periodo, estarán a cargo de los Gerentes y de las Juntas Directivas que determine el Alcalde Mayor y el Secretario de Salud respectivamente. Dicha designación se producirá al día siguiente de la entrada en vigencia del presente Acuerdo.

b). La designación de las Juntas Directivas de transición se hará exclusivamente de entre las Empresas Sociales del Estado objeto de la fusión.

c). Las juntas directivas de las Empresas Sociales del Estado objeto de la fusión se disolverán al día siguiente de la entrada en vigencia del presente Acuerdo.

d). Los Gerentes de las Empresas Sociales del Estado objeto de la fusión permanecerán como directores científicos durante el periodo de transición siempre y cuando sean profesionales del área de la salud y en el caso de que su profesión sea diferente, asumirá dicha dirección el profesional del área de la salud que le siga jerárquicamente. Sus funciones, durante este período, estarán orientadas, en forma exclusiva, a facilitar a los Gerentes y Juntas Directivas de transición las labores

derivadas de la subrogación de obligaciones y derechos, dispuesta en el presente Acuerdo.

e). Las Juntas Directivas de transición deberán durante este periodo, tramitar las autorizaciones requeridas ante la Superintendencia Nacional de Salud, aprobar los ajustes presupuestales, determinar la estructura organizacional, aprobar la planta de personal, los estatutos, el reglamento interno, los manuales de funciones y requisitos y el de procedimientos de las Empresas Sociales del Estado resultantes de la fusión.

f). Igualmente durante este periodo las juntas directivas de transición adelantarán el proceso para la elección de los gerentes definitivos de las Empresas Sociales del Estado resultantes de la fusión, los cuales deberán posesionarse en sus cargos al vencimiento del periodo de transición.

PARÁGRAFO. Las Juntas Directivas y los Gerentes deberán atender los parámetros señalados en la Ley 909 de 2004 al momento de adecuar, bajo su responsabilidad, la estructura organizacional y la planta de personal de las Empresas Sociales del Estado que resultan de la fusión.

ARTÍCULO 4º. Nuevas Juntas Directivas. Durante el periodo de transición a que hace referencia el artículo anterior, la Secretaría Distrital de Salud realizará las acciones correspondientes para la conformación de las nuevas juntas directivas de las ESE resultantes de la fusión.

Las Juntas Directivas de las Empresas Sociales del Estado resultantes de la fusión estarán compuestas por nueve (9) integrantes los cuales serán designados de conformidad con lo dispuesto por el Decreto 1876 de 1994 y los Acuerdos 13 y 17 de 1997 del Concejo Distrital de Bogotá.

ARTÍCULO 5º. Subrogación de derechos y obligaciones. Subrogar en las Empresas Sociales del Estado, que resultan de la fusión ordenada mediante el presente Acuerdo, las obligaciones y derechos de toda índole pertenecientes a las Empresas Sociales del Estado fusionadas.

Las Empresas Sociales del Estado que resulten de la fusión realizarán los ajustes presupuestales y financieros necesarios para el cabal cumplimiento de las obligaciones por ellas adquiridas.

Para efectos del cumplimiento del presente artículo y dentro del período de transición, el Gobierno Distrital, a través de las instancias correspondientes, con la coordinación de la Secretaría de Hacienda Distrital, efectuará las modificaciones presupuestales a que haya lugar.

ARTÍCULO 6º. Garantía de derechos. Las fusiones a las que se refiere el presente Acuerdo, se harán con plena garantía de los derechos laborales adquiridos, tanto individuales como colectivos, de trabajadores oficiales y empleados de carrera administrativa, igualmente se respetarán integralmente todas las convenciones colectivas de trabajo y acuerdos laborales vigentes.

En ningún caso, como resultado de la fusión, se suprimirán cargos de carrera administrativa ni empleos de trabajadores oficiales.

ARTÍCULO 7º. Contratación con terceros. Las Empresas Sociales del Estado creadas con el presente Acuerdo, exigirán y verificarán que las empresas o entidades contratistas respeten los derechos laborales de sus empleados.

CAPÍTULO. III

CREACIÓN DE NUEVAS ENTIDADES

ARTÍCULO 8º. Derogado por el art. 157, Acuerdo Distrital 761 de 2020.

El texto original era el siguiente:

ARTÍCULO 8. Creación de la Entidad Asesora de Gestión Administrativa y Técnica. Autorícese al Gobierno Distrital para que constituya una entidad mixta sin ánimo de lucro, de control y mayoría pública en su composición, organizada como corporación en los términos del artículo 96 de la Ley 489 de 1998, con autonomía administrativa y financiera, vinculada al sector salud del Distrito Capital y cuyo objeto social será el desarrollo de actividades de logística y de servicios no misionales como apoyo a la gestión de las Empresas Sociales del Estado del Distrito Capital.

ARTÍCULO 9º. Derogado por el art. 157, Acuerdo Distrital 761 de 2020.

El texto original era el siguiente:

ARTÍCULO 9. Funciones esenciales de la Entidad Asesora de Gestión Administrativa y Técnica. La entidad asesora de gestión administrativa y técnica desarrollará las siguientes actividades principales:
a). Adelantar acciones de inteligencia de mercados con el fin de identificar a nivel nacional e internacional las mejores prácticas y procesos administrativos relacionados con el funcionamiento de los prestadores de servicios de salud.
b). Asesorar el proceso de integración informática del sector salud en el Distrito Capital que incluya tanto a las entidades de aseguramiento como a las de prestación de servicios de salud.
c). Asesorar el proceso de compras conjuntas de insumos y medicamentos para las ESE del Distrito.
d). Asesorar para las ESE distritales los procesos de facturación, call center, agenciamiento de citas médicas por medios electrónicos, referencia y contra referencia de pacientes y negociación para la venta de servicios de salud.
e). Asesorar respecto a los servicios administrativos a cargo de las ESE en los cuales por economías de escala o estandarización de la calidad sea recomendable adelantar en forma conjunta.

f). Asesorar a las subredes de prestación de servicios de salud en la creación y puesta en marcha de mecanismos efectivos de defensa de los derechos de los usuarios en salud de conformidad con lo establecido en la ley.

g). Las demás actividades que señalen los estatutos y que sean conexas con su objeto social.

PARÁGRAFO 1. El Secretario Distrital de Salud definirá la gradualidad mediante la cual la Entidad Asesora de Gestión Administrativa y Técnica asumirá la asesoría de los aspectos señalados en el presente artículo.

PARÁGRAFO 2. En los estatutos de las Empresas Sociales del Estado se incorporará el régimen que regula el relacionamiento de tales empresas con la Entidad Asesora de Gestión Administrativa y Técnica, el cual será de obligatoria aplicación por parte de los gerentes de las ESE.

ARTÍCULO 10º. Integrantes de la Entidad Asesora de Gestión Administrativa y Técnica. Serán integrantes fundadores de la Entidad Asesora de Gestión Administrativa y Técnica las siguientes entidades:

a). El Distrito Capital que será representado por el Secretario de Salud Distrital.

b). Las Empresas Sociales del Estado del Distrito Capital representadas por sus gerentes.

c). Capital Salud EPS-S S.A.S, representada por su gerente.

d). Las entidades privadas sin ánimo de lucro que suscriban el acta de constitución.

Serán integrantes adherentes las demás entidades que se vinculen con posterioridad a la constitución de la Entidad y de conformidad con los requisitos establecidos en sus estatutos. En ningún caso podrán ser integrantes adherentes de la corporación entidades con ánimo de lucro.

ARTÍCULO 11º. Patrimonio de la Entidad Asesora de Gestión Administrativa y Técnica. El patrimonio de la entidad estará conformado por:

1. Los aportes iniciales y posteriores que hagan los miembros de la entidad, representados en dinero, bienes o servicios.

2. Los bienes adquiridos por concepto de donaciones, contribuciones, transferencias, herencias y legados de personas naturales o jurídicas, de entidades públicas, privadas o de economía mixta, y de organismos nacionales o extranjeros.

3. Las reservas legales, estatutarias y voluntarias que consagren la Ley y los Estatutos.

4. Los incrementos patrimoniales y los excedentes que obtenga por el ejercicio de sus actividades.

5. La valorización de activos, y cualquier otro ingreso susceptible de incrementar el patrimonio conforme a lo definido en los estatutos.

PARÁGRAFO 1. El Fondo Financiero Distrital de Salud realizará un aporte inicial por un valor de $5.000 millones de pesos para el sostenimiento de la entidad.

PARÁGRAFO 2. Serán principios de la Entidad Asesora de Gestión Administrativa y Técnica, los de transparencia, economía, responsabilidad, selección objetiva, planeación, igualdad, moralidad, eficiencia, celeridad, imparcialidad, publicidad, rendición de cuentas e independencia.

ARTÍCULO 12º. Principio de autosostenibilidad. La Entidad Asesora de Gestión Administrativa y Técnica funcionará bajo un principio de autosostenibilidad financiera. Su funcionamiento se financiará con los ingresos que perciba por las labores desarrolladas.

Los servicios prestados por la Entidad Asesora de Gestión Administrativa y Técnica serán remunerados por las entidades beneficiarias de su gestión y tal remuneración podrá consistir en un porcentaje de los ahorros obtenidos u otra diferente que se acuerde entre las partes.

ARTÍCULO 13º. Principio de transparencia. La Entidad Asesora de Gestión Administrativa y Técnica contará con un código de ética corporativa que regule tanto las relaciones de la entidad como las de sus colaboradores. Este código contendrá un régimen estricto de conflicto de intereses de modo que se garantice la transparencia de todas las actuaciones de la entidad.

ARTÍCULO 14º. Órganos de Dirección y Administración. La Dirección y Administración de la Entidad Asesora de Gestión Administrativa y Técnica estará a cargo de la Asamblea General, la Junta Directiva y el Gerente General en la forma que determinen los estatutos.

Tanto la Asamblea General como la Junta Directiva siempre deberán tener una composición mayoritaria por parte de entidades públicas del orden distrital.

ARTÍCULO 15º. Término de duración y disolución. La Entidad Asesora de Gestión Administrativa y Técnica tendrá una duración inicial de veinte (20) años que podrán prorrogarse por otro periodo igual por decisión de la asamblea general. Su disolución se producirá por las causales previstas en las leyes vigentes o por decisión de la asamblea general.

ARTÍCULO 16º. Liquidación de la Administración Pública Cooperativa. La Administración Pública Cooperativa a que hace referencia el Acuerdo 400 de 2009 se disolverá y liquidará y los excedentes, en caso de que los hubiere, serán restituidos a las Empresas Sociales del Estado del Distrito.

ARTÍCULO 17º. Creación del Instituto Distrital de Ciencia, Biotecnología e Innovación en Salud. Autorícese al Gobierno Distrital para que constituya una entidad mixta sin ánimo de lucro organizada como corporación y como entidad de ciencia y tecnología de las reguladas en el Decreto Ley 393 de 1991, con autonomía administrativa y financiera, vinculada al sector salud del Distrito Capital y cuyo objeto social será la realización de actividades de investigación, desarrollo e innovación relacionadas con medicina transfusional, terapia e ingeniería tisular y celular avanzada, medicina regenerativa, medicina de laboratorio y centro de formación del talento humano.

ARTÍCULO 18º. Funciones esenciales del Instituto Distrital de Ciencia, Biotecnología e Innovación en Salud. Modificado por el art. 102, Acuerdo 761 de 2020**.** <*El nuevo texto es el siguiente*> El Instituto Distrital de Ciencia, Biotecnología e Innovación en Salud –IDCBIS- desarrollará las siguientes actividades principales:

a). Fortalecer y fomentar una cultura ciudadana para la donación de sangre, componentes sanguíneos, órganos y tejidos humanos y células con propósitos de trasplante, medicina regenerativa o investigación.

b). Obtener, procesar, almacenar y distribuir componentes sanguíneos, tejidos y células humanas con propósitos de trasplante, medicina regenerativa o investigación.

c). Ofrecer servicios altamente especializados y de referencia, en banco de sangre, banco de tejidos humanos, banco de sangre de cordón umbilical, terapias avanzadas, medicina transfusional, medicina regenerativa y laboratorio de inmunología de transfusión y trasplantes.

d). Formar, capacitar y entrenar talento humano en las áreas de conocimiento desarrolladas por la entidad, con énfasis en investigación.

e). Gestionar líneas de investigación e innovación tecnológica en diversos campos de las ciencias de la salud humana, con énfasis en medicina transfusional, ingeniería tisular, terapias avanzadas y medicina regenerativa, en coordinación con centros académicos y de investigación nacionales e internacionales.

f). Servir como entidad asesora, consultora y de referencia, para entidades nacionales e internacionales en los aspectos relacionados con el desarrollo de su objeto social.

g). Desarrollar y gestionar un Registro de Donantes de Progenitores Hematopoyéticos, con propósitos de investigación y trasplante.

h). Desarrollar actividades encaminadas a la apropiación social del conocimiento en el área de la salud, así como la difusión de la ciencia. i). Las demás actividades que señalen los estatutos y que sean conexas con su objeto social.

El texto original era el siguiente.

ARTÍCULO 18º. Funciones esenciales del Instituto Distrital de Ciencia, Biotecnología e Innovación en Salud. *El Instituto Distrital de Ciencia, Biotecnología e Innovación en Salud –IDCBIS- desarrollará las siguientes actividades principales:*

a). Fortalecer y fomentar una cultura ciudadana para la donación de sangre, componentes sanguíneos, órganos y tejidos humanos y células con propósitos de trasplante, medicina regenerativa o investigación.

b). Obtener, procesar, almacenar y distribuir componentes sanguíneos, tejidos humanos y células madre con propósitos de trasplante, medicina regenerativa o investigación.

c). Ofrecer servicios centralizados, altamente especializados y de referencia, en banco de sangre, banco de tejidos humanos, banco de sangre de cordón umbilical, terapia celular, medicina transfusional, medicina regenerativa y laboratorio de inmunología de transfusión y trasplantes.

d). Formar, capacitar y entrenar talento humano en las áreas de conocimiento desarrolladas por la entidad, con énfasis en investigación.

e). Gestionar líneas de investigación e innovación tecnológica en diversos campos de las ciencias de la salud humana, con énfasis en medicina transfusional, ingeniería tisular, terapia celular avanzada y medicina regenerativa, en coordinación con centros académicos y de investigación nacionales e internacionales.

f). Servir como entidad asesora, consultora y de referencia, para entidades nacionales e internacionales en los aspectos relacionados con el desarrollo de su objeto social.

g). Las demás actividades que señalen los estatutos y que sean conexas con su objeto social.

ARTÍCULO 19º. Integrantes del Instituto Distrital de Ciencia, Biotecnología e Innovación en Salud. Serán integrantes fundadores del IDCBIS las siguientes entidades:

a). El Distrito Capital, representado por el Secretario de Salud Distrital.

b). Las Empresas Sociales del Estado del Distrito Capital representadas por sus gerentes.

c). Las entidades públicas, mixtas y privadas sin ánimo de lucro que suscriban el acta de constitución.

Serán integrantes adherentes las demás entidades que se vinculen con posterioridad a la constitución de la entidad y de conformidad con los requisitos establecidos en sus estatutos. En ningún caso podrán ser integrantes de la corporación entidades con ánimo de lucro.

ARTÍCULO 20º. Patrimonio del Instituto Distrital de Ciencia, Biotecnología e Innovación en Salud. El patrimonio del instituto estará conformado por:

1. Los aportes iniciales y posteriores que hagan los integrantes de la entidad, representados en dinero, bienes o servicios.

2. Los bienes adquiridos por concepto de donaciones, contribuciones, transferencias, herencias y legados de personas naturales o jurídicas, de entidades públicas, privadas o de economía mixta, y de organismos nacionales o extranjeros.

3. Las reservas legales, estatutarias y voluntarias que consagren la Ley y los Estatutos.

4. Los incrementos patrimoniales y los excedentes que obtenga por el ejercicio de sus actividades.

5. La valorización de activos, y cualquier otro ingreso susceptible de incrementar el patrimonio conforme a lo definido en los estatutos.

PARÁGRAFO 1. La totalidad del equipamiento tecnológico, biomédico y bienes muebles de toda índole, que actualmente se encuentren asignados al Hemocentro Distrital, harán parte del aporte del Distrito Capital para la constitución del IDCBIS.

PARÁGRAFO 2. Autorícese a la Administración Distrital para suscribir convenio de comodato, con el fin de posibilitar el uso por parte del IDCBIS, del espacio físico del Centro Distrital de Salud, donde actualmente funciona el Hemocentro Distrital.

PARÁGRAFO 3. El Fondo Financiero Distrital de Salud realizará un aporte inicial por un valor de $5.000 millones de pesos para el sostenimiento del Instituto.

ARTÍCULO 21º. Modificado por el art. 104, Acuerdo 761 de 2020. <*El nuevo texto es el siguiente*> **Financiación para el Fortalecimiento de la Investigación.** Las labores adelantadas por el Instituto serán remuneradas por las Empresas Sociales del Estado del orden distrital y por las demás entidades a las cuales le preste sus servicios. En todo caso, podrá recibir aportes del Distrito Capital para la financiación de sus proyectos específicos, así como otras fuentes como cooperación o transferencias del presupuesto nacional.

Parágrafo 1. El Instituto Distrital de Ciencia Biotecnología e Innovación en Salud deberá implementar sistemas integrados de gestión, planeación y calidad que conllevan a la ejecución eficiente de los recursos financieros aportados por el Distrito Capital.

Parágrafo 2. El IDCBIS dará prioridad a las solicitudes o necesidades que se presenten las ESES Distritales.

Parágrafo 3. El desarrollo de tecnologías y conocimientos producidos por el Instituto con recursos públicos o mixtos deberán estar a disposición de la Administración Distrital en condiciones especiales, con costos razonables y preferiblemente de manera gratuita, en virtud de la importancia para la formulación e implementación de política pública y en la medida que constituyen soluciones para la salud pública y el beneficio de la ciudadanía, siendo un asunto de interés público.

El texto original era el siguiente.

ARTÍCULO 21º. Principio de autosostenibilidad. *El Instituto Distrital de Ciencia, Biotecnología e Innovación en Salud funcionará bajo el principio de autosostenibilidad financiera. Su funcionamiento se financiará con los ingresos que perciba por las labores desarrolladas.*

Las labores adelantadas por el instituto serán remuneradas por las Empresas Sociales del Estado del orden Distrital y por las demás entidades a las cuales le preste sus servicios.

PARÁGRAFO. *El IDCBIS dará prioridad a las solicitudes o necesidades que presenten las ESES Distritales.*

ARTÍCULO 22º. Órganos de Dirección y Administración del IDCBIS. La Dirección y Administración del Instituto estará a cargo de la Asamblea General, la Junta Directiva y el Gerente General en la forma que determinen los estatutos.

La Asamblea General y la Junta Directiva tendrán una composición mayoritaria por parte de entidades públicas del orden distrital.

ARTÍCULO 23º. Término de duración y disolución del IDCBIS. El instituto tendrá una duración inicial de veinte (20) años, que podrá prorrogarse por otro periodo igual, por decisión de la asamblea general. Su disolución se producirá por las causales previstas en las leyes vigentes, los estatutos o por decisión de la asamblea general.

CAPÍTULO. IV

REORDENAMIENTO DE ORGANISMOS

ARTÍCULO 24º. Consejo Distrital de Seguridad Social en Salud Ampliado. La Administración Distrital, en el marco de sus competencias, reglamentará en el término de un año, la nueva composición y funciones del Consejo Distrital de Seguridad Social en Salud ampliando la participación actual e incorporando las funciones relacionadas en la Ley 1438 de 2011.

El Consejo Distrital de Seguridad Social en Salud será, el máximo organismo asesor del sector salud en el Distrito Capital y será la instancia de coordinación que posibilite la adecuada ejecución de las políticas públicas en salud.

ARTÍCULO 25º. Red integrada de servicios de salud. La oferta pública de prestación de servicios de salud, del Distrito Capital, se organizará en una Red Integrada de Servicios de Salud, que se estructura a través de cuatro subredes que correspondan a cada una de las ESAS resultantes de la fusión ordenada en el presente Acuerdo.

Las subredes se organizarán en servicios ambulatorios y hospitalarios en todos los niveles de complejidad.

PARÁGRAFO. La coordinación y articulación de la red integrada de servicios de salud se realizará a través de un Comité Directivo de Red integrado por el Secretario Distrital de Salud, los gerentes de cada una de las ESE, el gerente de Capital Salud EPS y el gerente de la Entidad Asesora de Gestión Administrativa y Técnica.

ARTÍCULO 26º. Creación de otros comités. La Administración Distrital conformará los comités sectoriales o intersectoriales que se requieran como instancias de coordinación y como instrumentos para el adecuado desarrollo de los cometidos estatales de responsabilidad del sector salud.

CAPÍTULO. V

PARTICIPACIÓN COMUNITARIA

ARTÍCULO 27º. Instancias de participación comunitaria. El proceso de reorganización del sector salud mantendrá las instancias de participación comunitaria existentes en el Distrito Capital. La composición de las juntas directivas de las ESES resultantes de la fusión se hará conforme a lo señalado en las normas vigentes sobre la materia.

ARTÍCULO 28º. Asociaciones de usuarios. Las asociaciones de usuarios de las ESES, objeto de la fusión se mantendrán en las ESES resultantes de la fusión y su ámbito de acción se concentrará en las unidades de prestación de servicios para las que se conformaron inicialmente, sin perjuicio que en ejercicio de su autonomía puedan optar por fusionarse.

ARTÍCULO 29º. Comités de Participación Comunitaria en Salud. Los COPACOS existentes se mantendrán en su ámbito de acción comunitaria a nivel de las localidades del Distrito Capital y la interacción con las ESES resultantes de la fusión se producirá en relación con las localidades que comprenden cada una de las Subredes integradas de prestación de servicios de salud.

ARTÍCULO 30º. Juntas Asesoras Comunitarias. Para fortalecer los espacios de participación comunitaria se conformará una junta asesora comunitaria por cada unidad de prestación de servicios de salud, regida por un Director Científico.

Cada junta asesora comunitaria estará conformada por siete (7) integrantes de los cuales dos (2) corresponderán a las asociaciones de usuarios de las unidades de prestación de servicios de salud, dos (2) a los COPACOS, dos (2) a las Asociaciones de Usuarios de las EPS y uno (1) como delegado de la Alcaldía Local del área de influencia de la unidad de prestación de servicios de salud. La elección de los seis

(6) integrantes de la comunidad, se realizará mediante un proceso democrático. El Director Científico de la unidad de prestación de servicios de salud será el responsable de la secretaría técnica de la Junta Asesora Comunitaria.

Las juntas asesoras comunitarias desarrollarán las siguientes actividades:

a). Canalizar y presentar al Director Científico de la unidad de prestación de servicios las razones de inconformidad más relevantes que la comunidad manifieste respecto de la calidad de los servicios.

b). Realizar propuestas de mejoramiento de los servicios de salud con base en los principales problemas detectados.

c). Canalizar y presentar al Director Científico de la unidad de prestación de servicios aquellos aspectos que influyan sobre los determinantes sociales de la salud en la respectiva área geográfica.

d). Servir de canal de comunicación ante la comunidad para la implementación y desarrollo de la política de atención integral en salud.

e). Participar activamente de las iniciativas de salud urbana, de promoción de la salud y de prevención de la enfermedad propuestas por la autoridad sanitaria e invitando a participar al resto de la población.

f). Asesorar y apoyar procesos de planeación, ejecución y evaluación de las acciones en salud que se desarrollen en su área de influencia.

g). Impulsar procesos de divulgación de información y rendición de cuentas ante la comunidad.

CAPÍTULO VI

SECTOR SALUD

ARTÍCULO 31º. Misión del Sector Salud. El Sector Salud tiene la misión de formular, adoptar, dirigir, planificar, coordinar, ejecutar y evaluar las políticas para el mejoramiento de la situación de salud de la población del Distrito Capital, mediante acciones en salud pública, prestación de servicios de salud y dirección del Sistema General de Seguridad Social en Salud.

ARTÍCULO 32º. Integración del Sector Salud. El Sector Salud está integrado por la Secretaría Distrital de Salud, cabeza del Sector, y las siguientes entidades y organismos:

Entidades Adscritas:

Establecimiento público: Fondo Financiero Distrital de Salud - FFDS,

Empresas Sociales del Estado: Subred Integrada de Servicios de Salud Sur E.S.E, Subred Integrada de Servicios de Salud Norte E.S.E., Subred Integrada de Servicios de Salud Sur Occidente E.S.E., Subred Integrada de Servicios de Salud Centro Oriente E.S.E.

Entidades con vinculación especial:

Sociedad de Economía Mixta: Capital Salud EPS-S S.A.S.

Entidad sin ánimo de lucro mixta: Entidad Asesora de Gestión Administrativa y Técnica.

Entidad sin ánimo de lucro mixta: Instituto Distrital de Ciencia, Biotecnología e Innovación en Salud.

Organismos:

Consejo Territorial de Seguridad Social en Salud.

Comité Directivo de Red.

ARTÍCULO 33º. Naturaleza, objeto y funciones básicas de la Secretaría Distrital de Salud. La Secretaría Distrital de Salud es un organismo del Sector Central con autonomía administrativa y financiera que tiene por objeto orientar y liderar la formulación, adecuación, adopción e implementación de políticas, planes, programas, proyectos y estrategias conducentes a garantizar el derecho a la salud de los habitantes del Distrito Capital.

Como organismo rector de la salud ejerce su función de dirección, coordinación, vigilancia y control de la salud pública en general del Sistema General de Seguridad Social y del régimen de excepción, en particular.

Además de las atribuciones generales establecidas en el Acuerdo 257 de 2006 para las secretarías, la Secretaría Distrital de Salud tiene las siguientes funciones:

a). Formular, ejecutar y evaluar las políticas, estrategias, planes, programas y proyectos del sector salud y del Sistema General de Seguridad Social en Salud de conformidad con las disposiciones legales.

b). Dirigir, coordinar, vigilar y controlar el sector salud y el Sistema General de Seguridad Social en Salud en Bogotá, D.C.

c). Vigilar y controlar el cumplimiento de las políticas y normas técnicas, científicas y administrativas que expida el Ministerio de Salud y Protección Social, para garantizar el logro de las metas del sector salud y del Sistema General de Seguridad Social en Salud, sin perjuicio de las funciones de inspección, vigilancia y control atribuidas a las demás autoridades competentes.

d). Administrar, controlar y supervisar los recursos propios, los cedidos por la Nación y los del Sistema General de Participaciones con destinación específica para salud y cualquier otro tipo de recursos que se generen con ocasión del cumplimiento de su naturaleza, objeto y funciones, garantizando siempre su correcta utilización, dentro del marco de la ley.

e). Gestionar y prestar los servicios de salud prioritariamente a través de su red adscrita, de manera oportuna, eficiente y con calidad a la población pobre no asegurada que resida en su jurisdicción, en lo no cubierto con subsidios a la demanda.

f). Realizar las funciones de inspección, vigilancia y control en salud pública, aseguramiento y prestación del servicio de salud.

g). Formular y ejecutar el plan de intervenciones colectivas y coordinar con los sectores y la comunidad las acciones que en salud pública se realicen para mejorar las condiciones de calidad de vida y salud de la población.

h). Coordinar, supervisar y controlar las acciones de salud pública que realicen en su jurisdicción las Entidades Promotoras de Salud - EPS, las entidades transformadas y adaptadas y aquellas que hacen parte de los regímenes exceptuados y especiales, así como las Instituciones Prestadoras de Servicios de Salud - IPS e instituciones relacionadas.

i). Promover el aseguramiento de toda la población con énfasis en la población más pobre y vulnerable, al Sistema General de Seguridad Social en salud de acuerdo con lo establecido en el ordenamiento jurídico.

j). Mantener actualizadas las bases de datos de la población afiliada al régimen subsidiado y reportar dichas novedades a la Secretaria de Planeación y demás entidades competentes.

k). Definir, vigilar y controlar la oferta de servicios de salud del Distrito Capital, con el fin de garantizar su calidad y funcionamiento según las necesidades de la población.

l). Promover el aseguramiento de las poblaciones especiales conforme lo define la ley y las acciones en salud pública establecidas en el ordenamiento jurídico.

m). Promover la coordinación de políticas con otros sectores, en particular hábitat, educación, planeación y medio ambiente, para incidir de manera integral en los determinantes de la salud y en la atención de la enfermedad.

n). Implementar programas de prevención del consumo del alcohol, del tabaco y otras drogas y de rehabilitación y desintoxicación.

ARTÍCULO 34º. Vigencia y derogaciones. El presente Acuerdo rige a partir de su publicación, modifica parcialmente el Acuerdo 257 de 2006 y deroga las disposiciones que le sean contrarias.

PUBLÍQUESE Y CÚMPLASE.
ROBERTO HINESTROSA REY
Presidente
HERNANDO ROJAS MARTÍNEZ

Secretario General de Organismo de Control (e.)

ALCALDÍA MAYOR DE BOGOTÁ, DISTRITO CAPITAL

PUBLÍQUESE Y EJECÚTESE

ENRIQUE PEÑALOSA LONDOÑO

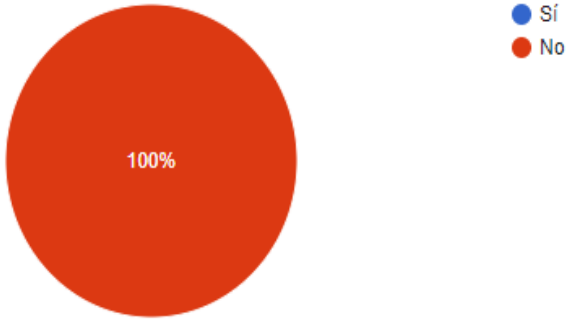
Alcalde Mayor de Bogotá, D.C.

Abril 6 de 2016

Anexo C: Resultado análisis de encuesta

La entidad cuenta con personal encargado exclusivamente a la seguridad de la Información?

5 respuestas

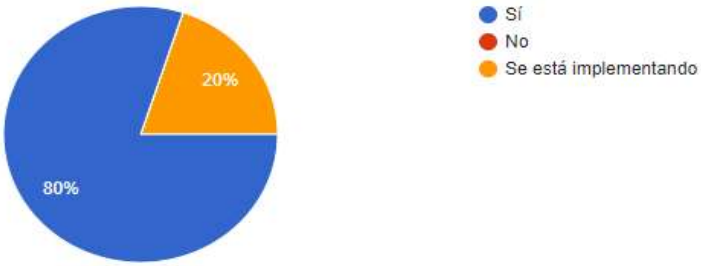


Se cuenta con un protocolo definido para la salida de información institucional (Archivos institucionales Historias clinicas, datos financieros, etc.), en dispositivos extraíbles o equipos de computo de terceros?

5 respuestas

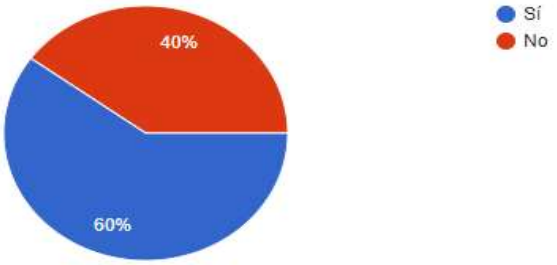
La entidad cuenta con Firewall o UTM, ya sea físico o por medio de software, para el control de acceso no deseado?

5 respuestas



Los equipos de computo portátiles, cuentan con VPN configurada para el uso fuera de la institución?

5 respuestas

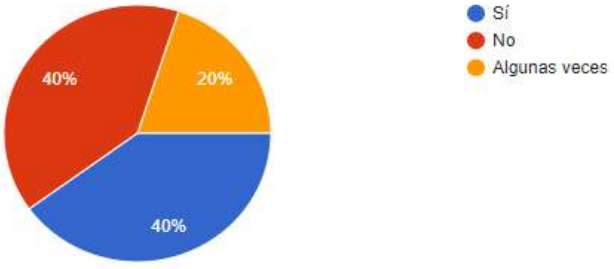


Se cuenta con inventario de equipos de computo, servidores, software, dispositivos de red y comunicaciones actualizado?

5 respuestas

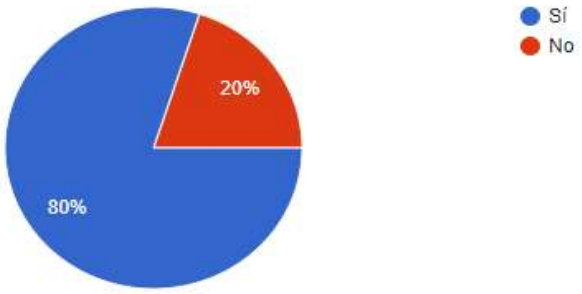
Ante una solicitud para unir un equipo de computo personal (ya sea de un funcionario asistencial o administrativo) a red institucional. Se realizan comprobaciones de Legalidad de Software, Antivirus Actualizado, Actualizaciones del sistema Operativo?

5 respuestas



Se han presentado incidentes de Seguridad que impliquen perdida de información?

5 respuestas



Se cuenta con un proceso de realización de Backups (Automático o Manual) a la información de dispositivos de usuario final de manera recurrente?

5 respuestas