ESE SAN VICENTE DE PAUL

Lorica – Córdoba

2023

POLITICA DE SEGURIDAD INFORMATICA

La ESE Hospital San Vicente de Paul de Lorica – Córdoba, se compromete a establecer la política y proceso de seguridad informática que tiene como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en la entidad.

INTRODUCCIÓN

En la actualidad la información del hospital se ha reconocido como un activo valioso y a medida que los sistemas de la información apoyan cada vez más los procesos de misión crítica se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos. Nuestra empresa, los sistemas y red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, fuego, robo e inundación. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes.

Con la actualización de la presente Política de Seguridad informática la E.S.E HOSPITAL SAN VICENTE DE PAUL formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales.

OBJETIVO

Mantener la Integridad, Disponibilidad, Privacidad, Control y Autenticidad de la información manejada por la ESE Hospital San Vicente de Paul de Lorica - Córdoba

PRINCIPIOS DE SEGURIDAD INFORMÁTICA

La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

- **CONFIDENCIALIDAD:** los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
- **INTEGRIDAD**: los componentes del sistema permanecen inalterados a menos que sean modificados por los usuarios autorizados.
- **DISPONIBILIDAD**: Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

Para ello es necesario considerar aspectos tales como:

- **PRIVACIDAD**: os componentes del sistema son accesibles solo por usuarios autorizados
- **CONTROL**: solo los usuarios autorizados deciden cuando y como permitir el acceso a la información
- **AUTENTICIDAD:** Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.
- **AUDITORÍA:** Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.

- **PROTECCIÓN A LA DUPLICACIÓN:** Los activos de información son objeto de clasificación, y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.
- **NO REPUDIO:** Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.
- **LEGALIDAD:** Los activos de información cumplen los parámetros legales, normativos y estatutarios de la institución.
- **CONFIABILIDAD DE LA INFORMACIÓN:** Es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad.

POLÍTICA DE SEGURIDAD INFORMATICA

E.S.E HOSPITAL SAN VICENTE DE PAUL DE LORICA

GENERALIDADES

La política de seguridad requiere no solamente conocer las amenazas a las que están expuestas la información y los recursos de una organización, sino también establecer el origen de las mismas, que pueden ser internas o externas a la organización.

De nada valdría proteger la empresa de los usuarios del exterior si también existen amenazas internas. Por ejemplo, si un usuario utiliza un disquete que contiene un virus podría expandirlo a toda la intranet.

Una política de seguridad es "la declaración de las reglas que se deben respetar para acceder a la información y a los recursos". Los documentos de una política de seguridad deben ser dinámicos, es decir, ajustarse y mejorarse continuamente según los cambios que se presentan en los ambientes donde se crearon.

Las políticas de seguridad se desarrollan con el fin de preservar la información y los sistemas de una Empresa, y garantizando la integridad, confidencialidad y

disponibilidad de la información. Los documentos relativos a las políticas de seguridad informática deben contemplar los procedimientos para hacer cumplir las reglas, las responsabilidades en todos los niveles. Todos ellos deben tener el apoyo gerencial de la organización.

Las políticas de seguridad informática deben ser conocidos por todo el personal de una organización.

En el contenido de los documentos deben estar claramente establecidos: El objetivo, los responsables del cumplimiento, las medidas que se aplicarán en caso de incumplimiento.

La información es un recurso que, como el resto de los activos, tiene valor para la Entidad y por consiguiente debe ser debidamente protegida.

El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad informática, garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la entidad apoyadas en un correcto sistema de información.

ORGANIZACIÓN PARA LA SEGURIDAD INFORMATICA

El Hospital San Vicente de Paúl garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad informática del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada Comité de **GESTION DE LA TECNOLOGÍA** cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- Coordinador (a) de la oficina de Calidad
- Coordinador (a) de la oficina de Planeación o un delegado especializado,

- Coordinador de la Oficina Asesora de Sistemas o un delegado especializado,
- Coordinador de la Red de Datos o un delegado especializado,
- Asesor certificado en seguridad de la información.

En todo caso, dicha comisión o la mesa de trabajo, deberá revisar y actualizar anualmente esta política presentando las propuestas a las directivas de la institución para su aprobación mediante resolución o acto jurídico correspondiente.

Los coordinadores de las dependencias, previa identificación y valoración de sus activos de información, hacen parte del grupo de responsable de Seguridad informática y por tanto deben seguir los lineamientos de gestión enmarcados en esta política y en los estándares, normas, guías y procedimientos recomendados por el Comité de Seguridad informática y aprobados por la gerencia.

Para la ejecución de esta política se tendrá en cuenta las siguientes condiciones:

1. Activar el servidor-Proxy para controlar el uso del internet a todos los equipos de cómputos y manejo de contenidos.
2. Adquirir antivirus conjunto con Anti spam para equipos de cómputos.
3. Realizar respaldo de la información cada día, semana o mes.
4. No descargar música, películas u otros archivos no legales
5. No abrir documentos adjuntos o hacer clic en enlaces de mensajes no solicitados
6. No visitar sitios web pornográficos o de contenido ilícito

7. No proporcionar datos personales a desconocidos por teléfono o e-mail

8. No utilizar la misma contraseña en diferentes páginas web o compartirlas

9. Excesiva y abusiva navegación por internet con fines extra laborales o no justificados por la tarea

10. Ocupación de memoria y demás recursos para fines personales

11. Descarga ilegal de software para fines personales

12. Descarga ilegal de música

13. Uso de correo electrónico para fines personales

14. Transmisión de sistemas o equipos informático.

15. Disponer de un plan de contingencia que contemple copias de resguardo, autenticación de usuarios, integridad de datos, confidencialidad de la información almacenada y control de acceso.

¿QUE ES UNA MESA DE SERVICIOS?

Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Deben existir procedimientos de monitoreo y escalamiento basados en los niveles de servicio acordados en los SLAs, que permitan clasificar y priorizar cualquier problema reportado como incidente, solicitud de servicio o solicitud de información. Medir la satisfacción del usuario final respecto a la calidad de la mesa de servicios y de los servicios de TI.

Es la ayuda que se presta a un usuario para apoyarlo en la búsqueda de la mejor solución a su problema de operación. El ámbito de acción tiene que ver con los procedimientos administrativos, la utilización de sistemas informáticos, la generación de resultados y el nivel de conocimientos. Se asume que aquí está inserta la infraestructura tecnológica.

En general se puede decir que el soporte lo solicita un usuario cuando no obtiene o no sabe cómo lograr los resultados deseados.

El requerimiento de soporte es casi siempre gatillado por una situación negativa para el usuario.

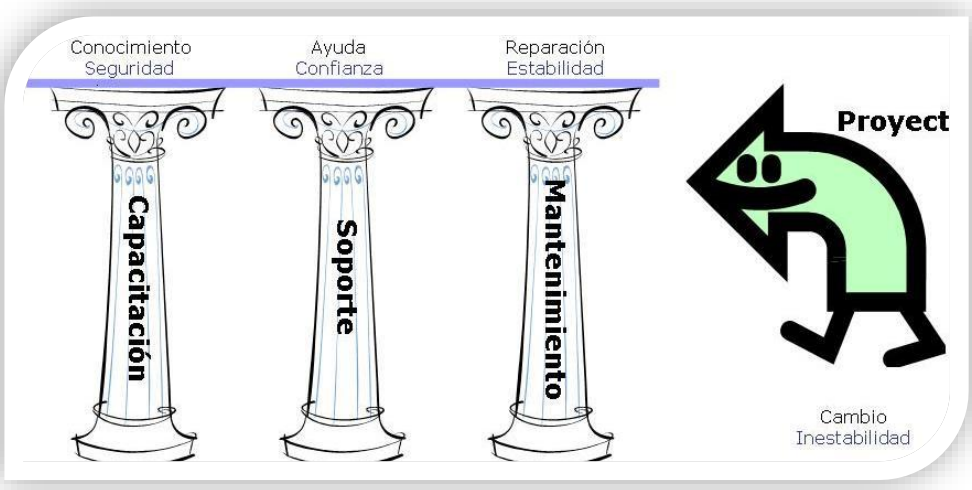
Está relacionado con la operación.

Por consiguiente, el Soporte es el apoyo o sostén que reciben los usuarios de parte del Área Informática para resolver los problemas de operación que se presentan con la utilización del software.

¿Qué esperan los Usuarios del Soporte?

En general, los Usuarios esperar en primer lugar que los Sistemas de Información sean perfectos, es decir siempre se comportar de una manera predeterminada y generar los resultados esperados, de hecho el software es percibido como algo inteligente, de modo que cuando falla, y la probabilidad que el software falle es igual a uno, genera un gran impacto emocional en el usuario, esto es porque los establecido, lo convencional y conocido tiene un comportamiento inesperado que saca al usuario de su rutina.

La situación anterior lleva a que un usuario en presencia de una falla necesita y quiere volver a la situación de normalidad lo antes posible y, es aquí donde el Área de Soporte juega un rol fundamental, ya que si está organizada y cuenta con los recursos adecuados es un generador de apoyo, de aquí el nombre de Soporte, de inapreciable valor para los usuarios.



Podemos ver que los elementos que generan seguridad, confianza y estabilidad son, respectivamente, la Capacitación, el Soporte y el Mantenimiento. Y, que la ejecución de proyectos, dado que necesariamente implica cambios provoca inestabilidad a los usuarios.

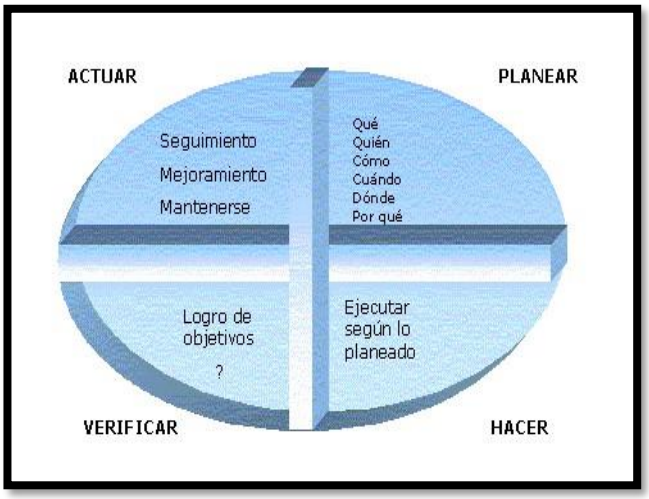
¿Cómo caracterizar un buen Soporte?

Las características de un buen Soporte son:

- Desde la perspectiva de un usuario.
- Facilidad para reportar el requerimiento.
- Prontitud en la solución de problema.
- Efectividad técnica.
- Seguridad en el servicio, no queda botado.
- Empatía.
- Formalidad.
- Seguimiento.
- Consideración con su opinión.
- Desde la perspectiva de Sistemas
- Niveles de Servicios Acordados y Publicados (tiempos, horarios, etc.)
- Entendimiento del requerimiento.
- Conocimientos informáticos y de los procesos de negocios.
- Procedimiento de Escalamiento.
- Un punto único de entrada de las solicitudes de soporte.
- Base de Conocimiento.
- Buena voluntad.

El Área de sistemas aplica las siglas Planificar (Plan), Hacer (Do), Verificar (Check) y Actuar (Act). esta metodología en la implementación de un sistema de gestión de la calidad, de tal manera que, al aplicarla en la política y objetivos de calidad, así como en la red de procesos, la probabilidad de éxito es mayor.

El resultado de la implementación de este ciclo permite al Área de sistemas una mejora integral de la competitividad, de los productos y servicios, mejorando continuamente la calidad, reduciendo los costes, optimizando la productividad, reduciendo los precios, incrementando la participación del mercado y aumentando la rentabilidad de la empresa u organización.



De manera adicional puede aplicarse a todos los procesos la metodología conocida como “Planificar- Hacer-Verificar-Actuar” (PHVA). PAVA puede describirse brevemente como:

- Planear: establecer los objetivos y los procesos necesarios para conseguir los resultados de acuerdo con los requisitos del cliente y las políticas de la organización.
- Hacer: implementar los procesos.
- Verificar: realizar el seguimiento y medición de los procesos y los productos y servicios respecto a las políticas, los objetivos y los requisitos para el producto.

PLAN DE SEGURIDAD

El objetivo del Plan de Seguridad es fijar los niveles de seguridad que han de ser incluidos como parte del SLAs, (**Acuerdo de Nivel de Servicio**)

Este plan ha de ser desarrollado en colaboración con la Gestión de Niveles de Servicio que es la responsable en última instancia tanto de la calidad del servicio prestado a los clientes como la del servicio recibido por la propia organización TI y los proveedores externos.

El Plan de Seguridad debe diseñarse para ofrecer un mejor y más seguro servicio al cliente y nunca como un obstáculo para el desarrollo de sus actividades de negocio.

- Siempre que sea posible deben definirse métricas e indicadores clave que permitan evaluar los niveles de seguridad acordados.

Un aspecto esencial a tener en cuenta es el establecimiento de unos protocolos de seguridad coherentes en todas las fases del servicio y para todos los estamentos implicados. "Una cadena es tan resistente como el más débil de sus eslabones", por lo que carece de sentido, por ejemplo, establecer una estricta norma de acceso si una aplicación tiene vulnerabilidades frente a inyecciones de SQL. Quizá con ello podamos engañar a algún cliente durante algún tiempo ofreciendo la imagen de "fortaleza" pero esto valdrá de poco si alguien descubre que la "puerta de atrás está abierta". servicio e informar los resultados.

Seguridad de la información en el Recurso Humano

Todo el personal de la E.S.E HOSPITAL SAN VICENTE DE PAUL, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe, debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. **EL Área de Sistemas** deben mantener un directorio completo y actualizado de tales perfiles.

El **Comité de Gestión de la Tecnología** determina cuales son los atributos que deben definirse para los diferentes perfiles.

El **Comité de Gestión de la Tecnología** debe elaborar, mantener, actualizar, mejorar y difundir el manual de "Responsabilidades Personales para la Seguridad de la Información en la E.S.E HOSPITAL SAN VICENTE DE PAUL.

La responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el jefe de departamento o supervisor del contrato; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

Responsabilidades del personal de la Empresa

Todo el personal de la E.S.E HOSPITAL SAN VICENTE DE PAUL, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y las tareas que desempeñe debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI (TECNOLOGIAS DE LA INFORMACION) y las reglas y perfiles que autorizan el uso de la información institucional.

Los procedimientos para obtener tales perfiles y las características de cada uno de

ellos deben ser mantenidos y actualizados por cada dependencia, de acuerdo a los lineamientos dados por el **área de sistemas**, en cuanto a la información que se utilice en la Red de Datos de la E.S.E, en cuanto a los **dispositivos** hardware y los elementos software.

El material idóneo de la empresa con una usabilidad indebida o ilegal, generará procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.

La Oficina de Recursos Humanos junto con el Área de Sistemas, se encargarán de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.

El Área de Sistemas se encargará de crear y mantener un centro documental de acceso general con información relacionada con temas de seguridad informática tales como responsabilidad en la administración de archivos, buenas prácticas, amenazas de seguridad, entre otros.

Responsabilidades de los Usuarios

Para poder usar los recursos de TI de la Entidad, los usuarios deben leer y aceptar un acuerdo con los términos y condiciones. **El Área de Sistemas,** debe asegurar los mecanismos para la difusión y aceptación de dichas condiciones por medio de registros y manuales en línea.

Se debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.

Responsabilidades de Usuarios Externos

Todos los usuarios externos y personal de empresas externas deben estar autorizados por un miembro del personal de la Entidad quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de TI institucionales. Los procedimientos para el registro de tales usuarios deben ser creados y mantenido por la **Oficina de Sistemas** en conjunto con la Oficina de Recursos Humanos.

Los usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI institucionales. Las cuentas de usuarios externos deben ser de perfiles específicos y tener caducidad no superior a **tres (2) meses**, renovables de acuerdo a la naturaleza del usuario, de igual manera aplica a los usuarios en los sistemas de información utilizados en la empresa.

Usuarios invitados y servicios de acceso público.

El acceso de usuarios no registrados solo debe ser permitido al sitio web de información institucional. El acceso y uso a cualquier otro tipo de recurso de información y TI no es permitido a usuarios invitados o no registrados.

AMENAZAS

Amenazas físicas

Dentro de las amenazas físicas podemos englobar cualquier error o daño en el hardware que se puede presentar en cualquier momento. Por ejemplo, daños en discos duros, en los procesadores, errores de funcionamiento de la memoria, etc. Todos ellos hacen que la información o no esté accesible o no sea fiable.

Otro tipo de amenazas físicas son las catástrofes naturales. Por ejemplo, hay zonas geográficas del planeta en las que las probabilidades de sufrir terremotos, huracanes, inundaciones, etc., son mucho más elevadas.

En estos casos en los que es la propia Naturaleza la que ha provocado el desastre de seguridad, no por ello hay que descuidarlo e intentar prever al máximo este tipo de situaciones.

Hay otro tipo de catástrofes que se conocen como de riesgo poco probable. Dentro de este grupo tenemos los Ataques nucleares, impactos de meteoritos, etc. y que, aunque se sabe que están ahí, las probabilidades de que se desencadenen son muy bajas y en principio no se toman medidas contra ellos.

Principales amenazas físicas de un sistema informático.

Tipos de amenazas físicas

Las amenazas físicas las podemos agrupar en las producidas por:

1. Acceso físico

Hay que tener en cuenta que cuando existe acceso físico a un recurso ya no existe seguridad sobre él. Supone entonces un gran riesgo y probablemente con un impacto muy alto.

A menudo se descuida este tipo de seguridad.

El ejemplo típico de este tipo es el de una organización que dispone de tomas de red que no están controladas, son libres.

2. Radiaciones electromagnéticas

Sabemos que cualquier aparato eléctrico emite radiaciones y que dichas radiaciones se pueden capturar y reproducir, si se dispone del equipamiento adecuado. Por ejemplo, un posible atacante podría 'escuchar' los datos que circulan por el cable telefónico.

Es un problema que hoy día con las redes wifi desprotegidas, por ejemplo, vuelve a estar vigente.

3. Desastres naturales

Respecto a terremotos el riesgo es reducido en nuestro entorno, ya que Colombia no es una zona sísmica muy activa. Pero son fenómenos naturales que si se produjeran tendrían un gran impacto y no solo en términos de sistemas informáticos, sino en general para la sociedad.

Siempre hay que tener en cuenta las características de cada zona en particular. Las posibilidades de que ocurra una inundación son las mismas en todas las regiones de Colombia. Hay que conocer bien el entorno en el que están físicamente los sistemas informáticos.

4. Desastres del entorno

Dentro de este grupo estarían incluidos sucesos que, sin llegar a ser desastres naturales, pueden tener un impacto igual de importante si no se disponen de las medidas de salvaguarda listas y operativas.

Puede ocurrir un incendio o un apagón y no tener bien definidas las medidas a tomar en estas situaciones o simplemente no tener operativo el SAI que debería responder de forma inmediata al corte de suministro eléctrico.

Amenazas lógicas

El punto más débil de un sistema informático son las personas relacionadas en mayor o menor medida con él. Puede ser inexperiencia o falta de preparación, o sin llegar a ataques intencionados propiamente, simplemente sucesos accidentales. Pero que, en cualquier caso, hay que prevenir.

Entre algunos de los ataques potenciales que pueden ser causados por estas personas, encontramos:

- **Ingeniería social:** consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían.
- **Shoulder Surfing:** consiste en "espiar" físicamente a los usuarios para obtener generalmente claves de acceso al sistema.
- **Masquerading:** consiste en suplantar la identidad de cierto usuario autorizado de un sistema informático o su entorno.
- **Basureo:** consiste en obtener información dejada en o alrededor de un sistema informático tras la ejecución de un trabajo.
- **Actos delictivos:** son actos tipificados claramente como delitos por las leyes, como el chantaje, el soborno o la amenaza.
- **Atacante interno:** la mayor amenaza procede de personas que han trabajado o trabajan con los sistemas. Estos posibles atacantes internos deben disponer de los privilegios mínimos, conocimiento parcial, rotación de funciones y separación de funciones, etc.

- **Atacante externo:** suplanta la identidad de un usuario legítimo. Si un atacante externo consigue penetrar en el sistema, ha recorrido el 80% del camino hasta conseguir un control total de un recurso.

5. Algunas amenazas lógicas

Las amenazas lógicas comprenden una serie de programas que pueden dañar el sistema informático. Y estos programas han sido creados:

- de forma intencionada para hacer daño: software malicioso o malware (malicious software)
- por error: bugs o agujeros.

Enumeramos algunas de las amenazas con las que nos podemos encontrar:

- **Software incorrecto**

  Son errores de programación (bugs) y los programas utilizados para aprovechar uno de estos fallos y atacar al sistema son los exploits. Es la amenaza más habitual, ya que es muy sencillo conseguir un exploit y utilizarlo sin tener grandes conocimientos.

- **Exploits**

  Son los programas que aprovechan una vulnerabilidad del sistema. Son específicos de cada sistema operativo, de la configuración del sistema y del tipo de red en la que se encuentren. Pueden haber exploits diferentes en función del tipo de vulnerabilidad.

- **Herramientas de seguridad**

  Puede ser utilizada para detectar y solucionar fallos en el sistema o un intruso puede utilizarlas para detectar esos mismos fallos y aprovechar para atacar el sistema. Herramientas como Nessus o Satan pueden ser útiles, pero también peligrosas si son utilizadas por crackers buscando información sobre las vulnerabilidades de un host o de una red completa.

- **Puertas traseras**

  Durante el desarrollo de aplicaciones los programadores pueden incluir 'atajos' en los sistemas de autenticación de la aplicación. Estos atajos se llaman puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos. Si estas puertas traseras, una vez la aplicación ha sido finalizada, no se destruyen, se está dejando abierta una puerta de entrada rápida.

- **Bombas lógicas**

  Son partes de código que no se ejecutan hasta que se cumple una condición. Al activarse, la función que realizan no está relacionada con el programa, su objetivo es completamente diferente.

- **Virus**

  Secuencia de código que se incluye en un archivo ejecutable (llamado huésped), y cuando el archivo se ejecuta, el virus también se ejecuta, propagándose a otros programas.

- **Gusanos**

  Programa capaz de ejecutarse y propagarse por sí mismo a través de redes, y puede llevar virus o aprovechar bugs de los sistemas a los que conecta para dañarlos.

- **Caballos de Troya**

  Los caballos de Troya son instrucciones incluidas en un programa que simulan realizar tareas que se esperan de ellas, pero en realidad ejecutan funciones con el objetivo de ocultar la presencia de un atacante o para asegurarse la entrada en caso de ser descubierto.

- **Spyware**

  Programas espía que recopila información sobre una persona o una organización sin su conocimiento. Esta información luego puede ser cedida o vendida a empresas

publicitarias. Pueden recopilar información del teclado de la víctima pudiendo así conocer contraseña o nº de cuentas bancarias o pines.

- **Adware**

  Programas que abren ventanas emergentes mostrando publicidad de productos y servicios. Se suele utilizar para subvencionar la aplicación y que el usuario pueda bajarla gratis u obtener un descuento. Normalmente el usuario es consciente de ello y da su permiso.

- **Spoofing**

  Técnicas de suplantación de identidad con fines dudosos.

- **Phishing**

  Intenta conseguir información confidencial de forma fraudulenta (conseguir contraseñas o pines bancarios) haciendo una suplantación de identidad. Para ello el estafador se hace pasar por una persona o empresa de la confianza del usuario mediante un correo electrónico oficial o mensajería instantánea, y de esta forma conseguir la información.

- **Spam**

  Recepción de mensajes no solicitados. Se suele utilizar esta técnica en los correos electrónicos, mensajería instantánea y mensajes a móviles.

- **Programas conejo o bacterias**

  Programas que no hacen nada, solo se reproducen rápidamente hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco, etc.).

6. Conformación de Claves y Usuarios (INFOTEC Y Seguridad de Paciente)

La conformación del usuario se establece bajo el siguiente esquema: Se coloca la primera letra del nombre + el primer apellido, en caso de usuarios comunes se coloca un número al final como consecutivo al usuario anterior

En la contraseña para ingresar a la plata forma de seguridad de paciente se colocará el número de cedula de ciudadanía o fecha de nacimiento y para el software de Infotec será '123' con las siguientes condiciones:

- El usuario tendrá que cambiar la contraseña inicial, para mayor recordación y control de su usuario
- El usuario debe establecer control de la plataforma del software al momento que termine de ingresar la información y cerrar su sesión para evitar manipulación de información de otros usuarios.
- En caso de pérdida de usuario o contraseña requerir por escrito para la verificación y se le asigna la contraseña como si fuera por primera vez

- Perfil del Usuario: El perfil de Usuario se establece bajo los niveles jerárquicos de la siguiente manera:
- Cada perfil determina los accesos a las diferentes opciones del programa
- Los accesos a las diferentes opciones del programa para cada perfil, son determinados por el administrador del sistema de acuerdo a las actividades a realzar

7. Rol de los usuarios:

se clasifica de la siguiente manera:

Programa de INFOTEC

- Usuario asistencial nivel 1 (Auxiliares de Enfermería y Jefes de Enfermería)
- Usuario asistencial nivel 2 (Médicos Generales y Especialistas)
- Usuario operativos nivel 1 (Áreas de Facturación)
- Usuarios operativos nivel 2 (Área de Auditorias)
- Usuarios operativos nivel 3 (Áreas Contables)
- Usuario administrador (Sistemas)

Programa de Seguridad del paciente

- Usuario estándar (reporta todas las áreas en general)
- Usuario Avanzado (coordinado de seguridad del Paciente)
- Administrador (Sistemas)

Recomendaciones:

- ✓ Divulgar la política de seguridad informática a todos los trabajadores de la E.S.E Hospital San Vicente de Paul de Lorica.
- ✓ Mantener copias de seguridad diarias de la base de datos del software Salud System y Seguridad del paciente.
- ✓ Acogerse a la circular emitida por gerencia a las áreas del área asistencial y Jefe Área logística. informar por escrito al área de Sistemas para desactivar las claves del sistema de información que se esté usando (área administrativa, área asistencial.) cuando no exista vinculación laboral con la institución, de igual forma para las personas que se vinculen laboralmente en la institución.
- ✓ Cambiar las contraseñas cada vez que salga un funcionario del hospital que haya tenido acceso a las mismas.
- ✓ Los correos donde se maneje información institucional deben ser entregados con su respectiva contraseña cuando la persona encargada ya no esté vinculado al hospital, por tal motivo no utilice correos personales para recibir y enviar información de la E.S.E Hospital San Vicente de Paul de Lorica.

BIBLIOGRAFÍA

1. https://apser.es/sla-informatica-lo-que-tienes-que-saber/
2. **http://192.168.1.100/wrgea/index.html -** Política de Seguridad del Paciente de Colombia
3. https://www.grupoacs.com/ficheros_editor/File/05_Compliance/Pol%C3%ADticas/31_Pol%C3%ADtica%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf
4. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008
5. http://www1.udistrital.edu.co:8080/c/document_library/get_file?uuid=46e3491d-3afd-4c99-8835-aaaf7faf435b&groupId=11808
6. www.esecamusantateresita.gov.com – Políticas de seguridad – 2012
7. https://www.camarahonda.org.co/wp-content/uploads/2017/09/POLITICADESEGURIDADDELAINFORMACION.pdf