UNIVERSIDAD DEL AZUAY

Facultad de Administración de Empresas

Escuela de Ingeniería de Sistemas y Telemática

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN APLICADAS AL HOSPITAL SANTA INÉS

Trabajo de graduación previo a la obtención del título de Ingeniera de Sistemas

Autor: Daniela Calderón Goercke

Director: Ing. Esteban Crespo

Cuenca, Ecuador

2013

DEDICATORIA

Agradezco a Dios, por haberme dado la vida y permitirme cumplir mis metas. A mis padres por siempre brindarme el apoyo y confianza para crecer como persona y lograr este objetivo profesional. A mis hermanos Moni y Pablo por acompañarme durante todo este camino y compartir juntos alegrías y fracasos.

AGRADECIMIENTOS

A todas las personas que ayudaron directa o indirectamente en la realización de este proyecto.

Especial agradecimiento a mi Director de Tesis Ing. Esteban Crespo por sus consejos y amistad.

DECLARACION DE AUTORIA

Yo, Daniela Calderón Goercke, declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

_____

Daniela Calderón Goercke

0104645320

Índice de Contenidos

RESUMEN

El propósito de este trabajo es desarrollar un documento con las Políticas de Seguridad de la Información para el Hospital Santa Inés, el mismo que consiste en identificar los activos de información que mantiene. El objetivo principal de la seguridad de la información es mantener la integridad, disponibilidad, privacidad, control de acceso y autenticidad de la información. Para la recolección de esta información se realizaron entrevistas personales con las cuales se obtuvo información acerca de software, hardware, los servicios, la edificación, las redes y datos del hospital. Luego se realizaron las Políticas de Seguridad de la Información y los planes de prueba, capacitación, control y retroalimentación.

La Seguridad de la Información del hospital Santa Inés tiene muchos puntos buenos y otros que se deben fortalecer. Mejorando estos puntos, el Hospital Santa Inés estaría asegurando de que la información se encuentra fuera de peligro.

ABSTRACT

The purpose of this work is to develop a document with the Information Security Policies for Santa Ines Hospital. The work consists on identifying the information assets that this institution maintains. The main goal of the information security is to maintain the integrity, availability, privacy, access control, and authenticity of the information.

In order to gather the information, personal interviews were carried out, which provided evidence regarding software, hardware, services, facilities, networks, and hospital data. Then, the Information Security Policies were developed as well as the plans for testing, training, control, and feedback.

The Information Security in Hospital Santa Ines has many good points and others that need improvement. If these points are improved, Santa Ines Hospital can be sure that the information is out of danger.

UNIVERSIDAD DEL
AZUAY
DPTO. IDIOMAS

Translated by,
Diana Lee Rodas

INTRODUCCION

El propósito de este trabajo es desarrollar un documento con las Políticas de Seguridad de la Información para el Hospital Santa Inés, el mismo que consiste en identificar los activos de información que mantiene dicha institución así como también los riesgos y amenazas que podrían alterar o perjudicar la información en ellos contenida.

La mayoría de personas que manejan la información desconocen el gran problema que podría provocar el daño o pérdida de esta, y no invierten en capital humano o económico para prevenirlo. El objetivo principal de la seguridad de la información es mantener la integridad, disponibilidad, privacidad, control de acceso y autenticidad de la información.

La seguridad informática es básica para cualquier tipo de empresa u organización, pero ¿De quién debemos protegernos? Se llama intruso a la persona que accede sin autorización a nuestro sistema, ya sea de forma intencional o no, y se clasifican según su nivel de conocimiento, pudiendo ser estos internos o externos a la institución. Pero los intrusos no son los únicos peligros, también están los desastres naturales, los daños en telecomunicaciones, en las redes internas, entre otros.

Las amenazas y ataques se pueden clasificar como ataques pasivos, en donde el atacante no altera la comunicación, sino solo escucha o monitoriza para obtener la información que está siendo transmitida; y ataques activos, donde el atacante modifica de alguna manera el flujo de datos.

Por todos estos daños se pretende realizar un manual con Políticas de Seguridad y tratar de mitigar todos los posibles riesgos y amenazas que podrían afectar a los activos de información, ya sea en este momento o en el futuro.

Capítulo 1

Marco teórico sobre las políticas de seguridad de la información

1.1 Que es Seguridad de la Información

La Seguridad de la Información son todas las medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e Integridad de la misma. La Seguridad de la Información no es lo mismo que la Seguridad Informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas. Se debe saber que los activos de información se enfrentan a varios peligros ya que puede ser divulgada, mal utilizada, ser robada, borrada o saboteada si no se tiene las precauciones necesarias . Esto afecta su disponibilidad y la pone en riesgo. (Gómez Vieites, 2007)

La información es poder y se clasifica como:

- **Crítica**: Es indispensable para el funcionamiento de la empresa.
- **Valiosa**: Es un activo importante y muy valioso.
- **Sensible**: Debe de ser conocida por las personas autorizadas.

Además existen dos conceptos muy importantes en lo que es la Seguridad de la Información:

- **Riesgo**: que es todo tipo de vulnerabilidades o amenazas que pueden ocurrir sin previo aviso y producir numerosas pérdidas para las empresas. Los riesgos más perjudiciales son a las tecnologías de información y comunicaciones.
- **Seguridad**: Es una forma de protección contra los riesgos.

La seguridad de la información comprende diversos aspectos entre ellos la disponibilidad, la comunicación, la identificación de problemas, el análisis de riesgos, la integridad, la confidencialidad y la recuperación de los riesgos. (Gómez Vieites, 2007)

1.2 Principios de la Seguridad de la Información

La seguridad de la información se fundamenta en tres principios:

1.2.1 Confidencialidad

Significa que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

1.2.2 Integridad

Se refiere al mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

1.2.3 Disponibilidad

Es la disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

1.3 Importancia de la Seguridad de la Información

En nuestro medio aún no existe una conciencia acerca de la importancia de la seguridad de la información, debido a que las personas no se ponen a pensar en qué pasaría si por un virus, o por la negligencia de un operador, o incluso un desastre natural, la información de un computador se pierde, y no hay manera de recuperarla, por esto es necesario prevenir estos posibles incidentes y saber cómo

actuar, y en caso de que no sea posible anticiparse tener un plan de contingencia. Cuando se presenta un ataque, la compañía se pone en desventaja frente a sus competidores, incluso, puede causar su cierre de operaciones si no responde con rapidez a las exigencias del mercado. Por ello, es vital para toda organización el aseguramiento de su información, proceso que debe ser acompañado permanentemente para conseguir resultados confiables.

Cabe destacar que la seguridad de los sistemas debido a la constante y acelerada evolución tecnológica, nunca será del cien por ciento; por ello aunque una compañía ya cuente con un sistema de seguridad informática, es necesario que sea probado o auditado por terceros, para descubrir sus niveles de vulnerabilidad, que entre otros, puede originarse al interior de la compañía.

1.4 Tretas y Vulnerabilidades de la Seguridad de la Información

1.4.1 Ataques

Los ataques o amenazas a un sistema son una violación de la información (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos identifican las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad. (Gonzalo Álvarez Marañón, 2000)

AMENAZAS

- Criminalidad (común y política)
  - Allanamiento, Sabotaje, Robo / Hurto, Fraude, Espionaje, Virus, ...

- Sucesos de origen físico
  - Incendio, Inundación, Sismo, Polvo Sobrecarga eléctrica, Falta de corriente, ...

- Negligencia y decisiones institucionales
  - Falta de reglas, Falta de capacitación, No cifrar datos críticos, Mal manejo de contraseñas, ...

Ilustración 1 Amenazas Fuente: (Erb)

El conocer las etapas que conforman un ataque informático da la ventaja de aprender a pensar como los atacantes y a no subestimar su mentalidad. Además se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque. Las cinco etapas que puede tener un ataque son: (Mieres, 2009)

Ilustración 2 Fases de un ataque Fuente (Mieres, 2009)

Reconocimiento: En esta etapa se obtiene información con respecto a la víctima, la misma que puede ser una persona o una organización. Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social, el Dumpster Diving (búsqueda de información valiosa en la basura), el sniffing entre otras técnicas. (Mieres, 2009)

Exploración: En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros. Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el network mappers, port mappers, network scanners, port scanners, y vulnerability scanner. (Mieres, 2009)

Obtener acceso: En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema descubiertos durante las fases de reconocimiento y exploración. Algunas de las técnicas que el atacante puede utilizar son ataques de Buffer Overflow (desbordamiento de buffer), de Denial of Service (Ataque de denegación de servicios DoS), Distributed Denial of Service (DDos), Password filtering y Session hijacking. (Mieres, 2009)

Mantener el acceso: Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos. (Mieres, 2009)

Borrar huella: Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS). (Mieres, 2009)

Es importante saber que existen cuatro categorías generales de amenazas o ataques, las mismas que consisten en:

- **Interrupción:** en donde un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros. (Gonzalo Álvarez Marañón, 2000)
- **Intercepción:** aquí una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Un ejemplo de este ataque es acceder a una línea para robar datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para descubrir la

identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad). (Gonzalo Álvarez Marañón, 2000)

- **Modificación:** en donde una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Por ejemplo cuando se cambian los valores en un archivo de datos, se altera un programa para que funcione de forma diferente o se modifica el contenido de los mensajes que están siendo transferidos por la red. (Gonzalo Álvarez Marañón, 2000)
- **Fabricación:** en donde una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Un ejemplo de este ataque es la introducción de mensajes falsos en una red o añadir registros a un archivo. (Gonzalo Álvarez Marañón, 2000)

Además estos ataques se pueden clasificar también en ataques pasivos y ataques activos.

1.4.1.1 Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad. (Gonzalo Álvarez Marañón, 2000)

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información. (Gonzalo Álvarez Marañón, 2000)

1.4.1.2 Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- **Suplantación de identidad:** el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta. (Gonzalo Álvarez Marañón, 2000)
- **Re actuación:** uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada. (Gonzalo Álvarez Marañón, 2000)
- **Modificación de mensajes:** una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje “Ingresa un millón de dólares en la cuenta A” podría ser modificado para decir “Ingresa un millón de dólares en la cuenta B”. (Gonzalo Álvarez Marañón, 2000)
- **Degradación fraudulenta del servicio:** impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes falsos. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc. (Gonzalo Álvarez Marañón, 2000)

1.4.2 Brechas de seguridad

1.4.2.1 Ingeniería Social

La Ingeniería Social son estrategias de ataque que se basan en el engaño y que están orientadas a explotar las debilidades del factor humano. Los atacantes saben cómo utilizar estas metodologías y lo han incorporado como elemento fundamental para llevar a cabo cualquier tipo de ataque. En la informática se refiere a la obtención de información sensible y/o confidencial de un usuario cercano a un sistema u organización explotando ciertas características que son propias del ser humano.

Las personas constituyen uno de los problemas más importantes de seguridad para cualquier organización porque a diferencia de los componentes tecnológicos, son el único elemento, dentro de un entorno seguro, con la capacidad de decidir "romper" las reglas establecidas en las políticas de seguridad de la información. Por ignorancia o negligencia, pueden permitir a un atacante obtener acceso no autorizado y de esta manera, podrá evitar los complejos esquemas y tecnologías de seguridad que se hayan implementado en la organización.

Por ejemplo, en este sentido, la confianza y la divulgación de información son dos de las debilidades más explotadas para obtener datos relacionados a un sistema. Como contramedida, la única manera de hacer frente a los métodos de Ingeniería Social es la educación. Absolutamente todas las personas que forman parte de la organización, desde la secretaria, los administradores de la red y todos, deben estar capacitados en cuanto a las debilidades y los métodos de engaño más empleados por los atacantes para que logren identificarlos y dar aviso de cualquier anomalía que se produzca en el equipo o en determinado ambiente. (Mieres, 2009)

1.4.2.2 Factor Insiders

Factor Insiders son los mismos empleados desde dentro de la Institución u Organización. Una de las formas más eficaces que posee un atacante para romper los esquemas de seguridad, es desde el interior de la organización. Por ejemplo, el atacante podría conseguir un empleo en la organización que desea atacar y obtener el suficiente nivel de confianza en la organización para luego explotar los puntos de acceso. Del mismo modo, cualquier integrante puede convertirse en un empleado disgustado y decidir robar información y causar daños como una forma de venganza. (Mieres, 2009)

Cuando este tipo de actos es cometido con intenciones de obtener beneficios económicos a través de información corporativa, es denominado Insiders Trading (comercio de personal interno). En cualquiera de los casos, muchas de las herramientas y medidas de seguridad que se implementen en el entorno informático no serán eficaces. (Mieres, 2009)

Una de las mejores soluciones es realizar auditorías continuas que incluyan monitoreo a través de programas keyloggers (registrador de teclas) que pueden ser por hardware o por software, mecanismos que impidan la instalación de programas por parte del personal, estricta configuración del principio de privilegios mínimos, des habilitación de puertos USB y prohibición del uso de dispositivos de almacenamiento extraíbles para evitar la fuga de información y entrada de otras amenazas como malware, si las computadoras forman parte de un dominio es necesario establecer políticas rigurosas en el Active Directory, entre otras. (Mieres, 2009)

1.4.2.3 Códigos maliciosos

Los códigos maliciosos, o malware, constituyen también una de las principales amenazas de seguridad para cualquier Institución y aunque parezca un tema trivial, suele ser motivo de importantes pérdidas económicas. Esta amenaza se refiere a programas que causan algún tipo de daño en el sistema informático. Dentro de esta categoría se incluyen los programas troyanos, gusanos, virus

informáticos, spyware, backdoors, rootkits, keyloggers, entre otros. Actualmente, casi el 80% de los ataques informáticos llevados a cabo por códigos maliciosos, se realizan a través de programas troyanos. Este tipo de malware ingresa a un sistema de manera completamente oculta activando una carga dañina, denominada payload, que despliega las instrucciones maliciosas. [1]

La carga dañina que incorporan los troyanos pueden ser, instrucciones diseñadas para destruir algún sector del disco rígido, eliminar archivos, registrar las pulsaciones que se escriben a través del teclado, monitorear el tráfico de la red, entre muchas más. Los atacantes utilizan troyanos de manera combinada junto a otros tipos de códigos maliciosos. Por ejemplo, cuando han conseguido acceso a través del troyano, implantan en el sistema otros códigos maliciosos como rootkits que permite esconder las huellas que el atacante va dejando en el equipo (Covering Tracks), y backdoors para volver a ingresar al sistema cuantas veces considere necesario; todo, de manera remota y sin que, en la mayoría de los casos, los administradores de la red adviertan su actividad.

Los troyanos necesitan ser ejecutados por el usuario. Es por ello que estas amenazas se plantan por medio de diferentes tecnologías como dispositivos USB, mensajería instantánea, redes P2P, e-mail, etcétera; a través de alguna metodología de engaño (Ingeniería Social), aparentando ser programas inofensivos como protectores de pantalla, tarjetas virtuales, juegos en flash, entre otros. Las contramedidas para prevenir ataques a través de este tipo de amenazas, son la implementación de programas antivirus que operen bajo mecanismos de detección avanzados. (Mieres, 2009)

1.4.2.4 Contraseñas

Otro de los factores comúnmente explotados por los atacantes son las contraseñas. Aunque ahora existen sistemas de autenticación complejos, las

[1] Informe sobre malware en América Latina, Laboratorio ESET Latinoamérica

contraseñas siguen, y seguirán, siendo una de las medidas de protección más utilizadas en cualquier tipo de sistema informático. En este tipo de proceso, llamado de factor simple, la seguridad del esquema de autenticación radica inevitablemente en la fortaleza de la contraseña y en mantenerla en completo secreto, siendo potencialmente vulnerable a técnicas de Ingeniería Social cuando los propietarios de la contraseña no poseen un adecuado nivel de capacitación que permita prevenir este tipo de ataques.

Si el entorno informático solo tiene protección mediante sistemas de autenticación simple, la posibilidad de ser víctimas de ataques de cracking o intrusiones no autorizadas es bastante grande. La solución ante este problema es la creación de contraseñas mucho más largas. Sin embargo, esta estrategia sigue siendo poco efectiva, simplemente, porque el personal no se encuentra preparado para recordar largas cadenas de caracteres y terminan escribiéndolas en lugares visibles o sitios accesibles por cualquier otra persona.

Otros problemas que suelen ser aprovechados por los atacantes son:

- La utilización de la misma contraseña en varias cuentas y otros servicios.
- Acceder a recursos que necesitan autenticación desde lugares públicos donde los atacantes pueden haber implantado programas o dispositivos físicos como keyloggers que capturen la información.
- Utilización de protocolos de comunicación inseguros que transmiten la información en texto claro como el correo electrónico, navegación web, chat, etcétera.
- Técnicas como surveillance (videoconferencia) o shoulder surfing (mirar por detrás del hombro), entre otras tantas, que permiten evadir los controles de seguridad.

Una medida para fortalecer este aspecto de la seguridad, es posible implementar mecanismos más robustos como “autenticación fuerte de doble factor”, donde no sólo se necesita contar con la contraseña sino que también es necesario algo que se tiene, como por ejemplo una llave electrónica USB o una

tarjeta que almacene certificados digitales para que a través de ellos se pueda validar o no el acceso de los usuarios a los recursos de la organización. (Mieres, 2009)

1.4.2.5 Configuraciones predeterminadas

Las configuraciones por defecto, tanto en los sistemas operativos, las aplicaciones y los dispositivos implementados en el ambiente informático, conforman otra de las debilidades que comúnmente son poco atendidas por pensar erróneamente que se tratan de factores triviales que no se encuentran presentes en la lista de los atacantes. Pero, las configuraciones predeterminadas hacen del ataque una tarea sencilla para quien lo ejecuta ya que es muy común que las vulnerabilidades de un equipo sean explotadas a través de códigos exploit donde el escenario que asume dicho código se basa en que el objetivo se encuentra configurado con los parámetros por defecto.

Por lo tanto, para mitigar y prevenir problemas de seguridad en este aspecto, y que muchas veces se omite, es simplemente cambiar los valores por defecto. (Mieres, 2009)

1.4.2.6 OSINT (Open Source Intelligence)

Los atacantes, aprenden constantemente técnicas de ataque que le permiten penetrar los esquemas de seguridad por más complejos que sean. Una de las primeras fases de un ataque informático, es la recolección de información a través de diferentes técnicas como discovery, footprinting o Google Hacking; y precisamente, Open Source Intelligence (Inteligencia de fuentes abiertas) se refiere a la obtención de información desde fuentes públicas y abiertas. La información recolectada por el atacante, no es más que una detallada investigación sobre el objetivo. Un atacante gasta la mayor parte de su tiempo en actividades de reconocimiento y obtención de información ya que cuanto más aprende el atacante sobre el objetivo, más fácil será llevar a cabo con éxito el ataque.

En la mayoría de los casos, las empresas brindan una enorme cantidad de datos sin darse cuenta. Los responsables de las organizaciones se sorprenderían al ver la cantidad de información que se puede encontrar en Internet tanto de las actividades propias de la organización, como, información sobre las actividades de los empleados y su familia. Aquí están algunos ejemplos concretos sobre el tipo y sensibilidad de la información que un atacante podría obtener haciendo OSINT:

- Los nombres de sus altos jefes y de cualquier empleado pueden ser obtenidos desde comunicados de prensa.
- La dirección de la empresa, números telefónicos y números de fax desde diferentes registros públicos o directamente desde el sitio web.
- Qué, o cuáles, empresas proveen el servicio de Internet (ISP) a través de técnicas sencillas como DNS lookup y traceroute.
- La dirección del domicilio del personal, sus números telefónicos, currículum vitae, datos de los familiares, puestos en los que desempeña funciones, antecedentes penales y mucho más buscando sus nombres en diferentes sitios.
- Los sistemas operativos que se utilizan en la organización, los principales programas utilizados, los lenguajes de programación, plataformas especiales, fabricantes de los dispositivos de networking, estructura de archivos, nombres de archivos, la plataforma del servidor web y mucho más.
- Debilidades físicas, accesspoint, señales activas, endpoint, imágenes satelitales, entre otras.
- Documentos confidenciales accidentalmente, o intencionalmente, enviados a cuentas personales de personas que no en la actualidad no guardan relación alguna con la organización, más allá del paso por la misma.
- Vulnerabilidades en los productos utilizados, problemas con el personal, publicaciones internas, declaraciones, políticas de la institución.

- Comentarios en blogs, críticas, jurisprudencia y servicios de inteligencia competitiva.

Como se ve, no hay límite a la información que un atacante puede obtener desde fuentes públicas abiertas donde, además, cada dato obtenido puede llevar al descubrimiento de más información. (Mieres, 2009)

1.5 Revisión macro ISO 27001

ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) es un estándar internacional para la seguridad de la información que fue aprobado y publicado en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. (libnova)

ISO/IEC 27001 es la única norma internacional auditable que define los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI). La norma fue creada para garantizar una selección de controles de seguridad adecuados y proporcionales. (Esplandiú)

Aquí se especifican los requisitos necesarios para establecer, implementar, operar monitorear, revisar, mantener y mejorar un SGSI según el conocido “Ciclo de Deming” o PDCA, que es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart. Las siglas PDCA son el acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

Modelo PDCA o PHVA aplicado a los procesos SGSI

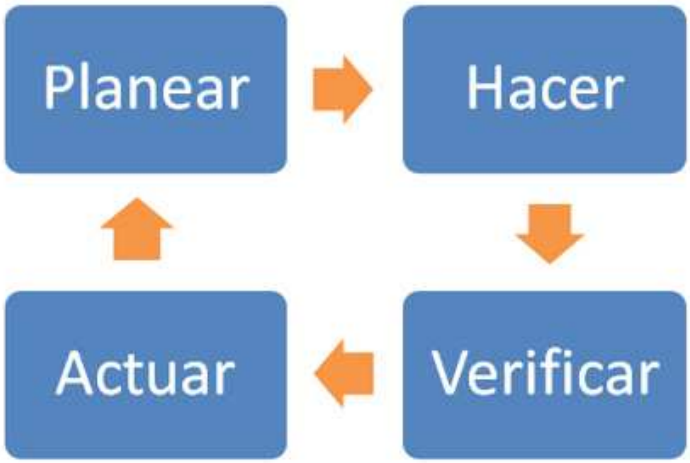

Ilustración 3 Modelo PDCA o PHVA aplicado a los procesos SGSI. Fuente: (Borrego, 2009)

Planificar: es donde se establecen las políticas, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos de la organización. (Internacional, 2005)

Hacer: se implementan y operan las políticas, controles, procesos y procedimientos SGSI. (Internacional, 2005)

Verificar: donde se evalúa y se mide el desempeño del proceso en comparación con las políticas, objetivos y experiencias prácticas SGSI y luego se reportan los resultados a la gerencia para su revisión. (Internacional, 2005)

Actuar: tomar acciones correctivas y preventivas, basadas en los resultados de la auditoria interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

Todo esto nos ayuda a proteger los activos de información y dar mayor confianza a cualquiera de las partes interesadas, sobre todo a los clientes. ISO/IEC 27001 es una norma adecuada para cualquier organización, grande o pequeña, de cualquier sector o parte del mundo. (Internacional, 2005)

Beneficios de la ISO 27001

- Mejora del conocimiento de los sistemas de información, sus problemas y los medios de protección.
- Mejora de la disponibilidad de los materiales y datos.
- Protección de la información
- Diferenciación sobre la competencia y mercado
- Algunas licitaciones internacionales empiezan a solicitar una gestión ISO 27001
- Reducción de los costos vinculados a incidentes
- Posibilidad de disminución de las primas de seguro. (Internacional, 2005)

La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, al que va a estar sometido al Sistema de Gestión de la Seguridad de la Información elegido. En general, es recomendable la ayuda de consultores externos. Aquellas organizaciones que hayan adecuado previamente de forma rigurosa sus sistemas de información y sus procesos de trabajo a las exigencias de las normativas legales de protección de datos o que hayan realizado un acercamiento progresivo a la seguridad de la información mediante la aplicación de las buenas prácticas de ISO/IEC 27002, partirán de una posición más ventajosa a la hora de implantar ISO/IEC 27001. (Internacional, 2005)

El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática generalmente Ingenieros o Ingenieros Técnicos en Informática, derecho de las nuevas tecnologías, protección de datos y sistemas de gestión de seguridad de la información. (Internacional, 2005)

Establecer y manejar el SGSI

Para establecer el SGSI la organización debe hacer lo siguiente:

1. Definir el alcance y los límites del SGSI en términos de las características del negocio, su ubicación, activos, tecnología, etc. (Internacional, 2005)
2. Definir una política SGSI en términos de las características del negocio, su ubicación, activos y tecnología que:
    a. Incluya un marco referencial para establecer sus objetivos y establezca un sentido de dirección general y principios para la acción con la relación a la seguridad de la información.
    b. Se tome en cuenta los requerimientos comerciales y legales o reguladores, y las obligaciones de la seguridad contractual
    c. Este alineada con el contexto a la gestión riesgo estratégico de la organización en la cual se dará el establecimiento y mantenimiento del SGSI.
    d. Establezca el criterio con el que se evaluara el riesgo
    e. Haya sido aprobada por la gerencia. (Internacional, 2005)
3. Definir el enfoque del costo del riesgo de la organización
    a. Identificar una metodología de cálculo del riesgo adecuado para el SGSI y los requerimientos identificados de seguridad, legales y reguladores de la información comercial.
    b. Desarrollar los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables. (Internacional, 2005)
4. Identificar los riesgos
    a. Identificar los activos dentro del alcance del SGSI y los propietarios de estos activos
    b. Identificar las amenazas para los activos

c. Identificar las vulnerabilidades que podrían ser explotadas por las amenazas

d. Identificar los impactos que pueden tener la pérdida de confiabilidad, integridad y disponibilidad sobre los activos. (Internacional, 2005)

5. Analizar y evaluar el riesgo

a. Aquí se calcula el impacto comercial sobre la organización que podría resultar de una falla en la seguridad.

b. Calcular la probabilidad realista de que se cumpla una de estas amenazas y vulnerabilidades.

c. Calcular los niveles de riesgo

d. Determinar si el riesgo es aceptable o requiere tratamiento. (Internacional, 2005)

6. Identificar y evaluar las opciones para el tratamiento de los riesgos, donde podemos:

a. Aplicar los controles aplicados

b. Aceptar los riesgos consiente y objetivamente, siempre que satisfagan las políticas y el criterio de aceptación del riesgo

c. Transferir los riesgos comerciales asociados a otras entidades

d. Seleccionar objetivos de control y controles para el tratamiento de riesgo

e. Obtener la aprobación de la gerencia para los riesgos residuales propuestos

f. Obtener la autorización de la gerencia para implementar y operar el SGSI

g. Preparar un manual de aplicabilidad (Internacional, 2005)

1.6 MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgos de la Seguridad de Información) fue elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. Esta metodología es útil para los que trabajan con información mecanizada y los sistemas informáticos que la tratan. Conocer el riesgo al cual se enfrentan los elementos de trabajo es imprescindible para poder gestionarlos y es por esto que han aparecido muchas guías y herramientas de soporte las cuales buscan objetivar el análisis y así saber que tan seguras o inseguros son.

Esta metodología es interesante para todos quienes trabajan con información digital y sistemas informáticos. Si esta información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es importantísimo para poder gestionarlos. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

MAGERIT persigue los siguientes objetivos:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

La ventaja de MAGERIT es que las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles. Mientras que la desventaja es que el hecho de tener que traducir de forma directa todas las valoraciones en valores económicos hace que

la aplicación de esta metodología sea realmente costosa. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

1.6.1 La metodología de MAGERIT es la siguiente:

Ilustración 4 Metodología Magerit Fuente: (Armando)

La realización de este plan de seguridad no se lograría sin la ayuda activa de las personas involucradas en el sistema de seguridad, por eso es necesaria la creación de un "cultura de seguridad", donde se debe concientizar a todos los involucrados de las necesidades. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

Para la creación de esta cultura se necesita:

- Una política de seguridad corporativa que se entienda, que se difunda y se mantenga al día.
- Y una formación continua a todos los niveles, según las responsabilidades de cada uno.

Y para que todas estas actividades se cumplan correctamente, es importante y necesario que la seguridad sea fácil de entender, que facilite el cumplimiento de las prácticas propuestas y sobre todo que sea practicada por la dirección. Para la realización del análisis y la gestión de riesgos hay dos tareas a realizar que son:

Análisis de riesgos, esta es una aproximación para determinar el riesgo siguiendo estos pasos:

1. Determinar los activos relevantes para la organización, su interrelación y su valor, en caso de que este fallara.
2. Determinar a qué amenazas están expuestos estos activos
3. Determinar que salvaguardas hay y que tan eficaces son frente al riesgo.
4. Estimar el impacto.
5. Estimar el riesgo. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

La siguiente figura muestra este recorrido:

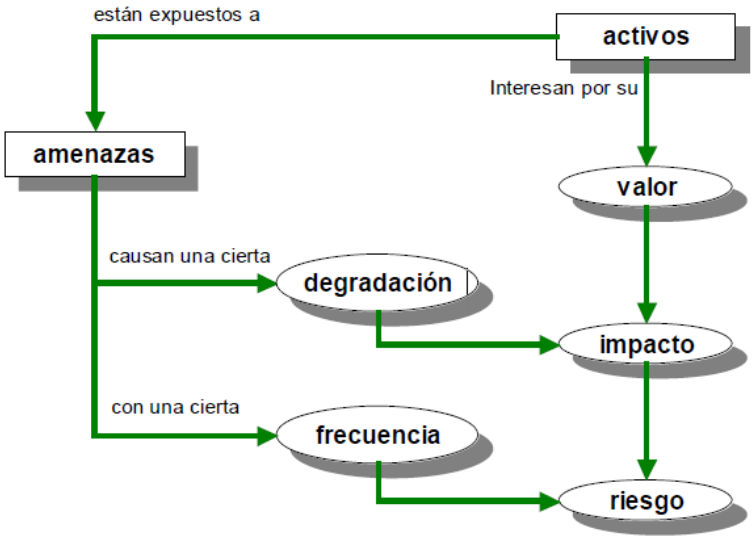

Ilustración 5 Recorrido del análisis de riesgos. Fuente: (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

Paso 1: Levantamiento de Activos de Información

Los activos son recursos del sistema de información o relacionados con este, necesarios para que la organización funcione correctamente y alcance sus objetivos. El activo principal es la información que maneja el sistema y alrededor de este hay otros activos importantes. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

Paso 2: Amenazas

El siguiente paso es determinar las amenazas que pueden afectar a cada activo de información. Pueden ser producidos por eventos naturales (terremotos, inundaciones), desastres industriales (contaminación), amenazas causadas por personas como errores o ataques intencionados. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

Cuando un activo es víctima de una amenaza se debe estimar cuan vulnerable es, en dos sentidos:

- Degradación: es cuan perjudicado resultaría el activo, mide el daño causado por un incidente en el supuesto de que ocurriera. Cuando las amenazas no son intencionales basta con calcular la pérdida proporcional de valor que se pierde. Pero si la amenaza es intencional no se puede pensar en proporcionalidad ya que el atacante puede causar mucho daño. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)
- Frecuencia: cada cuanto se materializa la amenaza. Pone en perspectiva la degradación, ya que la amenaza puede ser de terribles consecuencias pero de muy improbable materialización, mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulado un daño considerable. Los valores típico de la frecuencia son:

100	Muy frecuente	A diario
10	Frecuente	Mensualmente
1	Normal	Una vez al año
1/10	Poco frecuente	Cada varios años

Cuadro 1: (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

Paso 4: Determinación del impacto

Impacto es la medida de daño sobre el activo derivado de la materialización de una amenaza. Como ya conocemos el valor de los activos y la degradación que causan las amenazas, es directo determinar el impacto que estas tendrían en el sistema.

Hay dos tipos de impactos:

- El **impacto acumulado** que es el calculado teniendo en cuenta: su valor acumulado, que es su propio valor más el acumulado de los activos que dependen de él, y las amenazas a las que está expuesto. El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)
- El **impacto repercutido** es el calculado sobre un activo teniendo en cuenta: su valor propio y las amenazas a que están expuestos los activos de los que depende. El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

Paso 5: Determinación del riesgo

El riesgo es la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es fácil determinar el riesgo teniendo en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

Hay dos tipos de riesgos:

- El r**iesgo acumulado** que es calculado sobre un activo teniendo en cuenta el impacto acumulado sobre un activo debido a una amenaza y la frecuencia de la amenaza. El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la frecuencia de la amenaza. El riesgo acumulado, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)
- El **riesgo repercutido** que es calculado sobre un activo teniendo en cuenta el impacto repercutido sobre un activo debido a una amenaza y la frecuencia de la amenaza. El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la frecuencia de la amenaza. El riesgo repercutido, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

Paso 3: Salvaguardas

Las salvaguardas o contra medidas son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se eliminan simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otras seguridad física y, por último, está la política de personal. Las salvaguardas entran en el cálculo del riesgo de dos formas:

reduciendo la frecuencia de las amenazas y limitando el daño causado. Las salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar. La salvaguarda ideal es 100% eficaz, lo que implica que:

- es teóricamente idónea
- está perfectamente desplegada, configurada y mantenida
- se emplea siempre
- existen procedimientos claros de uso normal y en caso de incidencias
- los usuarios están formados y concienciados
- existen controles que avisan de posibles fallos

Entre una eficacia del 0% para aquellas que están de adorno y el 100% para aquellas que son perfectas, se estimará un grado de eficacia real en cada caso concreto. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

1.6.2 Gestión de Riesgos

El análisis de riesgos determina impactos y riesgos. Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé. En cambio el riesgo pondera la probabilidad de que ocurra. El impacto refleja el daño posible, mientras que el riesgo refleja el daño probable. Si el impacto y el riesgo residuales son despreciables, se ha terminado. Si no, hay que hacer algo. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

Para seleccionas las amenazas hay que planificar el conjunto de salvaguardas más aptas para detener tanto el impacto como el riesgo, reduciendo bien la degradación del activo (minimizando el daño), bien reduciendo la frecuencia de la amenaza (minimizando sus oportunidades). (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

Para toda amenaza hay que:

- Establecer una política de la organización al respecto; o sea, unas directrices generales de quién es responsable de cada cosa.
- Establecer una norma; o sea, unos objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada.
- Establecer unos procedimientos; o sea, instrucciones paso a paso de qué hay que hacer.
- Desplegar salvaguardas técnicas que efectivamente se enfrenten a las amenazas con capacidad para conjurarlas.
- Desplegar controles que permitan saber que todo lo anterior está funcionando según lo previsto.

A este conjunto de elementos se le conoce bajo el nombre de Sistema de Gestión de la Seguridad de la Información (SGSI), aunque se está gestionando tanto como actuando. Todo esto se resume en el desarrollo de una política, unas normas y unos procedimientos junto con el despliegue de una serie de salvaguardas y controles y, ahora sí verificar que todas y cada una de las amenazas tienen una respuesta adecuada. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

1.6.2.1 Tipos de salvaguardas

Se debe considerar varios tipos de salvaguardas:

- Salvaguardas preventivas que buscan que la amenaza no ocurra o su daño sea despreciable, impidiendo incidentes o ataques. Esto no siempre es posible ya que no es fácil predecir lo que va a suceder.
- Salvaguardas técnicas: en aplicaciones, equipos y comunicaciones
- Salvaguardas físicas: protegiendo el entorno de trabajo de las personas y los equipos
- Medidas de organización: de prevención y gestión de las incidencias

- Política de personal: política de contratación, formación permanente, organización de reportes de incidencias, plan de reacción y medidas disciplinarias. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

1.7 Clasificación y control de activos de seguridad

Los activos más importantes son:

- Los servicios: que se pueden prestar gracias a aquellos datos, y los que se necesitan para poder gestionar dichos datos.
- Las aplicaciones informáticas (software): que permiten manejar los datos.
- Los equipos informáticos (hardware): que son dispositivos de almacenamiento de los datos.
- Los soportes de información: dispositivos de almacenamiento de datos.
- Equipamiento auxiliar: que complementa el material informático.
- Las redes de comunicación: permiten el intercambio de datos.
- Las instalaciones: que acogen equipos informáticos y de comunicaciones.
- Las personas: que explotan u operan todos los elementos anteriormente citados. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

A estos activos se les debe clasificar según su especie, para luego darles una valoración, no de lo que cuesta en dinero sino de cuánto vale dentro de la organización para fines estratégicos corporativos. La dependencia entre activos es importante ya que los datos y los servicios dependen de los equipos, las comunicaciones y sobre todo de las personas, y esto podría provocar que un activo superior se vea afectado por un incidente de seguridad de uno inferior. (López Crespo Francisco, Magerit II Catalogo de Elementos - Version 2, 2006)

Aunque cada empresa organiza sus activos según sus circunstancias, con frecuencia se puede estructurar los activos en capas, donde las superiores dependen de las inferiores:

De un activo puede ser importante valorar las diferentes dimensiones:

- Su autenticidad: que causaría no saber exactamente quien hace o ha hecho cada cosa. Valoración típica de servicios y de datos.
- Su confidencialidad: que daño causaría si llegara a manos de quien no debe. Valoración típica de datos.
- Su integridad: que perjuicio causaría que estuviera dañado. Valoración típica de datos que pueden estar manipulados.
- Su disponibilidad: que causaría no tenerlo o no poder usarlo. Valoración típica de servicios.
- La trazabilidad del uso del servicio: que causaría no saber a quién se le presta tal servicio.
- La trazabilidad del acceso a los datos: que causaría no saber quién accede a qué dato y qué hace con ellos. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

Una vez determinadas las dimensiones que interesan de un activo hay que valorarlo, este es el valor que implicaría salir de una incidencia que destrozara el activo. Los factores a valorar son:

- Costo de reposición: adquisición e instalación.
- Costo de mano de obra invertida en recuperar el activo.
- Lucro cesante: pérdida de ingresos.
- Capacidad de operar: confianza de los usuarios y proveedores.
- Sanciones por incumplimiento de la ley u obligaciones contractuales.
- Daño a otros activos.
- Daño a personas.
- Daños medioambientales.

Esta valorización puede ser cuantitativa (con una cantidad numérica) o cualitativa (en una escala de niveles). Los criterios más importantes son la homogeneidad, compara valores aunque sean de diferentes dimensiones para así poder combinar propios y acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra, y la relatividad, que es importante poder relativizar el valor de un activo en comparación con otros activos. Estos criterios se satisfacen con valoraciones económicas.

Las escalas cualitativas permiten avanzar rápidamente, poniendo el valor de cada activo en un orden relativo respecto a los demás. Mientras que las valoraciones cuantitativas cuestan mucho esfuerzo, pero no sufren por las cualitativas. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

1.8 Políticas, planes y procedimientos de seguridad

Las políticas de Seguridad son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro y en algunos casos fuera de la organización. Una política de seguridad para que sea efectiva, necesita contar con elementos indispensables que apoyen este proceso: la cultura organizacional, las herramientas y el monitoreo. Esto involucra la participación directa y comprometida de las personas, el diseño de planes de capacitación constante a los usuarios. La disponibilidad de recursos financieros, técnicos y tecnológicos es fundamental y sobre todo actividades de control y retroalimentación que diagnostiquen e identifiquen puntos débiles para fortalecerlos siguiendo las mejores prácticas. (Clavijo, 2006)

Las políticas deben ser claras, concisas, contextualizadas a una realidad, enfocadas a las formas de hacer negocios de la empresa. Este documento debe ser entendido y no aprendido a todos los niveles, desde el personal operario hasta los altos mandos (directores, gerentes, etc.) Una Política de Seguridad es como la "carta de presentación de la empresa" donde se exponen los puntos que quiere dar a conocer la empresa, ¿a qué se dedica?, ¿qué quiere lograr?, ¿bajo qué

método trabaja?, ¿Cómo lo quiere lograr? Estas 4 preguntas son la estructura que debe de llevar la carta de presentación ante el cliente, el cual al leer estos 4 puntos va a tener una idea muy clara de la empresa a la que está a punto de comprar sus productos o servicios. (Clavijo, 2006)

1.8.1 La Gestión de la Seguridad

Para que los procesos de seguridad sean eficientes requieren de la participación de todos los miembros de la empresa. La gestión de la seguridad incluye una adecuada evaluación de riesgos, la asignación de recursos y otras actividades sistemáticas, tales como las auditorías internas, el control de las operaciones y las evaluaciones periódicas relativas a la seguridad. (Clavijo, 2006)

1.8.2 La persona responsable de la Seguridad

Esta persona debe tener un control absoluto sobre los procedimientos de seguridad implementados ya que es quien asume la responsabilidad de su funcionamiento. Esta persona debe tener los conocimientos precisos de todas las actividades que lleva a cabo la empresa, con el fin de establecer las medidas de seguridad requeridas, por lo que debe ser una persona equilibrada y de confianza. Se debe exigir de esta persona el secreto profesional, lo que es una garantía más. (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

1.8.3 La Administración o Gestión de riesgos

Para una eficiente y correcta gestión de los riesgos a los que están expuestos todos los procesos de nuestra organización, se deben cubrir todos los procesos involucrados en: identificar, evaluar y calificar los riesgos, tomando acciones para mitigar o anticiparlos, monitorear y revisar el progreso de su administración.

Entre los métodos más empleados para identificar riesgos se encuentran:

- Las listas de chequeo

- Juicios basados en la experiencia y registros
- Diagramas de flujo
- Lluvia de ideas
- Análisis de Sistemas
- Análisis de escena (López Crespo Francisco, Magerit I Metodo - Version 2, 2006)

1.8.4 El Control de los procesos

Controlar un proceso quiere decir cómo se controlan variables inherentes para:

- Reducir la variabilidad del producto final
- Incrementar la eficiencia
- Reducir impacto ambiental
- Mantener el proceso dentro de los límites de seguridad que corresponda (Vignoni, 2002)

El control de proceso consta de tres acciones fundamentales que son:

1. **Establecimiento de la directriz de control:** esta se establece sobre los fines y medios de un proceso. A este punto también se le llama Planeamiento de la Calidad, ya que la finalidad del control es garantizar, siempre, la satisfacción de las necesidades de las personas. (Vignoni, 2002)
2. **Mantenimiento de nivel de control:** si se cumplieron todos los estándares establecidos en la etapa anterior, resultará una calidad estándar, un costo estándar, una moral estándar y una seguridad estándar. Siempre que ocurran desvíos se deberá:
   - Actuar en el resultado para poner de nuevo el proceso en funcionamiento en forma inmediata. Por ejemplo: se quemó el motor - cambiar el motor
   - Actuar en la causa para prevenir la reaparición del desvío. Por ejemplo: Se quemó el motor. -¿Por qué se quemó el motor?

   Existen dos tipos de causas:

- **Causas específicas:** Se descubre la causa a través del análisis de las fallas, se actúa y se registra un informe. Por ejemplo: desvío en la calidad de la pieza debido al desgaste de la herramienta.
- **Causas crónicas:** En este caso es necesario realizar un análisis de proceso. Por ejemplo: Desvío en la calidad de la pieza debido a un defecto en el montaje de las máquinas. (Vignoni, 2002)

3. **Alteración de la directriz de control (mejoras):** En este mundo todo cambia constantemente. Cambian las necesidades de las personas, las materias primas, la tecnología, etc. Por lo tanto la directriz de control debe alterarse constantemente a fin de garantizar la Supervivencia. (Vignoni, 2002)

1.9 Gestión de incidentes de seguridad

La Gestión de Incidentes tiene como objetivo resolver cualquier incidente que cause la interrupción en el servicio de la manera más rápida y eficaz posible. Los objetivos principales de la Gestión de Incidentes son:

- Detectar cualquiera alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio según se define en el SLA (Acuerdo de Nivel de Servicio) correspondiente. (Amparo)

Según el libro de Soporte del Servicio de ITIL un incidente es:

"Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo". (Amparo)

Por lo que casi cualquier llamada al Centro de Servicios puede clasificarse como un incidente, lo que incluye a las Peticiones de Servicio tales como concesión de nuevas licencias, cambio de información de acceso, etc. siempre que estos servicios se consideren estándar.

Los principales beneficios de una correcta Gestión de Incidentes incluyen:

- Mejorar la productividad de los usuarios.
- Cumplimiento de los niveles de servicio.
- Mayor control de los procesos y monitorización del servicio.
- Optimización de los recursos disponibles.
- Una base de datos de gestión de configuraciones más precisa pues se registran los incidentes en relación con los elementos de configuración.
- Y principalmente: mejora la satisfacción general de clientes y usuarios.

Por otro lado una incorrecta Gestión de Incidentes puede acarrear efectos adversos tales como

- Reducción de los niveles de servicio.
- Se gastan valiosos recursos: demasiada gente o gente del nivel inadecuado trabajando concurrentemente en la resolución del incidente.
- Se pierde valiosa información sobre las causas y efectos de los incidentes para futuras reestructuraciones y evoluciones.
- Se crean clientes y usuarios insatisfechos por la mala y/o lenta gestión de sus incidentes.

(Amparo)

1.10 Gestión de continuidad del negocio

"Proceso de gestión holístico que identifica las amenazas potenciales de una organización y los impactos que pueden causar en las operaciones del negocio si esas amenazas se materializan. Además proporciona un marco de trabajo para construir una organización más resistente con capacidad para responder de forma efectiva y proteger los intereses de las partes interesadas clave, su reputación, imagen de marca y actividades de valor añadido" (ISO, 2012)

Para la Gestión de continuidad del negocio se establece la norma ISO 22301. Esta norma fue redactada por los principales especialistas en el tema y

proporciona el mejor marco de referencia para gestionar la continuidad del negocio en una organización. Si se implementa correctamente, la gestión de la continuidad del negocio disminuirá la posibilidad de ocurrencia de un incidente disruptivo y, en caso de producirse, la organización estará preparada para responder en forma adecuada y, de esa forma, reducir drásticamente el daño potencial de ese incidente. Esta norma puede ser implementada por cualquier organización, grande o pequeña, privada o pública (Kosutic)

ELEMENTOS DEL CICLO DE VIDA DE GESTION DE CONTINUIDAD DEL NEGOCIO (BCM)

Ilustración 6 Continuidad del Negocio. Fuente: (Cuate, 2011)

Esta gestión de continuidad es importante ya que los incidentes que ocurren en nuestro negocio o entorno pueden frenar o incluso paralizar nuestra actividad, impactando directamente en nuestros clientes y en los procesos críticos del

negocio. Un BCM (Gestión de Continuidad del Negocio) permite revisar constantemente los riesgos del negocio y conocer el grado real de preparación para responder ante situaciones imprevistas, ayudando a minimizar el impacto en el negocio de las posibles interrupciones. (Cruz, 2012)

Capítulo 2

Análisis de la situación real de la Seguridad de la Información del Hospital Santa Inés

En este capítulo se presenta un análisis de la situación actual del hospital Santa Inés el cual es necesario para la elaboración de las políticas y estándares de seguridad de la información que en un futuro nos permitirá proteger los activos de información de amenazas como desastres naturales, errores de hardware, software, intencionados o no intencionados por mal uso, divulgación o destrucción no autorizada.

El hospital Santa Inés, actualmente es uno de los más reconocidos en nuestra ciudad, ya que cuenta con excelente personal, sus equipos de medicina son de última tecnología, y su infraestructura también. Pero esto no es todo lo necesario para que el Hospital funcione en un cien por ciento ya que se deja de lado una parte muy importante que es la información que se maneja internamente, y por eso es que es necesario realizar un manual con Políticas de Seguridad y luego capacitar al personal con el mismo.

Aquí se incluirán varios puntos importantes que pasan desapercibidos por la alta dirección, el personal administrativo y el personal médico. Estas amenazas pueden provocar problemas si no son gestionadas de forma correcta. El objetivo principal es que los pasos contenidos en este documento sirvan de referente en cualquier situación de contingencia, que todo el personal lo lea y sepa que se debe hacer y que no se debería hacer, ya que la información es el activo más importante que el Hospital tiene como por ejemplo sus historias clínicas, la información de los pacientes, sus exámenes, información financiera, etc.

Por todo lo mencionado anteriormente es necesario diseñar un documento de Políticas de Seguridad de la Información, en donde se determine de forma clara, el cómo, el quién y cuándo se deben ejecutar las tareas asegurando de este modo que con la aplicación de éstos procedimientos se minimizará el riesgo de pérdida o alteración de información.

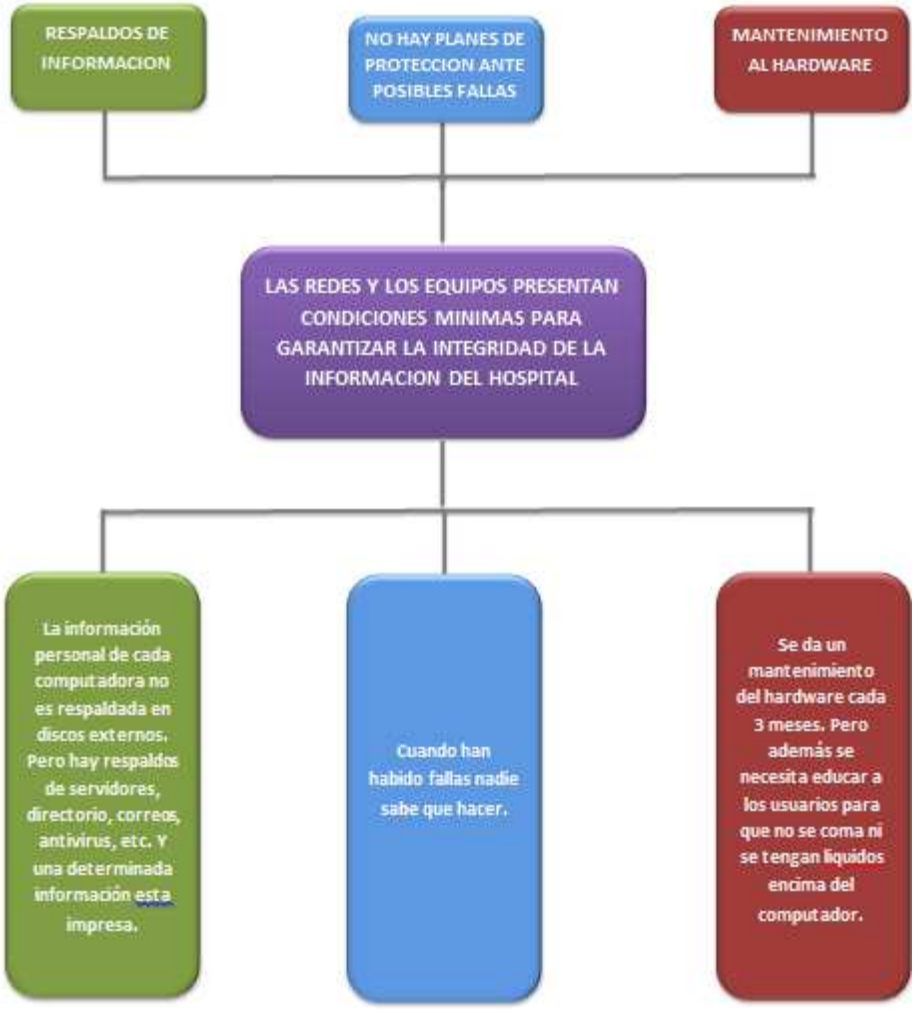

Grafico 1: Árbol de problemas, diagrama de causa y efecto

Para la recolección de información se realizaron entrevistas personales (Anexo 1) con las cuales se obtuvo información acerca de software, hardware, los servicios, la edificación, las redes y datos del hospital. Se utilizó el método de observación de cómo trabaja el personal, sobre la señalización y los elementos de seguridad ante un desastre natural, entre otros.

Para empezar con el análisis se abordará el tema del software, ya que hoy en día las aplicaciones se han convertido en una parte imprescindible de las empresas, y si son llevadas correctamente generan muchos beneficios. El Hospital

Santa Inés maneja un sistema interno, en el cual se almacena y verifica la información de todos los departamentos, contabilidad, financiero, botica, caja médica, UCI (Unidad de Cuidados Intensivos), farmacia, quirófano, etc. En este sistema cada usuario cuenta con permisos y contraseñas personales y únicamente tienen acceso a su área de trabajo para de esta manera poder evitar fraudes, suplantación de la identidad, pérdida de información siendo más fácil el control por que cada persona se hace responsable de la información que maneja.

Pero el software no es únicamente el sistema que manejan sino todos los programas que se utilizan. Dentro del hospital tiene como antivirus Kapersky el cual tiene una licencia comercial para 75 equipos con un período de vigencia de dos años, y con respecto al office ahora utiliza Microsoft Office pero la tendencia es cambiar este paquete ofimático a Open Office que es un procesador de texto multiplataforma, y es gratis. En el Centro de Cómputo se encuentran varios equipos informáticos, cada uno asignado a una tarea, el servidor de mail funciona con send mail, se cuenta con Dovecot que es un servidor de IMAP y POP3 de código para sistemas Linux, pensando en la seguridad.

Hay tres DVR con sistema operativo Linux que manejan el sistema de cámaras de seguridad del hospital, desde donde se monitorean las actividades del personal, pacientes y visitantes al edificio, y se graba automáticamente. Los registros de recursos de servicios SRV (SeRVice) son registrados en otro servidor. Y el firewall que bloquea o permite el paso de información desde el exterior a la red LAN y viceversa.

El acceso a Internet se encuentra controlado desde el centro de cómputo los usuarios tienen bloqueadas determinadas páginas, existe únicamente un correo electrónico interno en la clínica, con el cual si necesitan enviar un mail fuera se necesita un permiso especial, los usuarios tienen prohibido descargar juegos o aplicaciones a las computadoras, ya que la instalación de aplicaciones en las computadoras únicamente lo puede hacer el personal del departamento de sistemas.

Con respecto a los respaldos los usuarios no tiene almacenada ninguna información de sus computadores personales, pero si existen respaldos del sistema de servidores, de correos, del proxy, del directorio activo, de los sistemas clínico contable, antivirus, de cámaras de seguridad. Toda esta información se graba desde una oficina que se encuentra en el quinto piso y donde se encuentran los servidores. Pero a pesar de toda esta información respaldada la cantidad de información en papel es inmensa en algunos departamentos, lo que sería una pérdida total en caso de un incendio por ejemplo.

En el grupo hardware se incluyen a los servidores, a los que se les da un mantenimiento cada tres meses, este es un tiempo prudente, pero a las estaciones de trabajos, el departamento de mantenimiento solo limpia los CPU cada vez que los mismos se dañan por lo que tienden a llenarse de polvo y sobrecalentarse. Pero esta no es la única forma de cuidar el hardware ya que a veces nos damos cuenta del daño que podríamos causar al comer o tomar alimentos cerca del computador, o incluso fumar, lo cual debería estar prohibido. Por eso es necesario crear conciencia en el personal sobre estos temas y así ser proactivos ante estas situaciones.

Otro problema con los cables es que generalmente se encuentran enredados en los pies de los usuarios y esto también es un punto que se debe tomar en cuenta ya que se podría tropezar y desconectar los equipos y producir daño, por eso es importante que el usuario este consiente de esto y trate de mantenerlos en orden. En cuanto a los suministros de papel y tóner de la impresora los usuarios esperan hasta cuando se termina y ahí recién piden o buscan solucionar el problema, pero esto también debería ser previsto y así nunca se pararía el trabajo.

En lo que es edificación el Hospital Santa Inés cuenta con una de las mejores infraestructuras, esto es ascensor principal, el ascensor para el personal y las personas hospitalizadas, con las gradas principales y las gradas de emergencia, con puertas eléctricas que se abren y cierran automáticamente. La señalización y los extintores se encuentran distribuidos por el hospital de manera adecuada.

El Centro de Cómputo se encuentra en el quinto piso junto con la dirección médica del hospital y la gerencia que es lo recomendable, sin embargo es el último piso, y sobre el Centro de Cómputo está la terraza, que podría en algún momento filtrar el agua lluvia y llevarla directamente a las instalaciones del Centro de procesamiento de datos. El acceso de personal al Centro de Cómputo o de cualquier departamento no se maneja ningún tipo de control lo que hace que no se registren eventos en el acceso al mismo.

Para mitigar estas vulnerabilidades se debería contar con un plan de actividades a realizar ante estos fallos, para poder actuar ante eventos de negación de servicio ya sea por un virus, robo, desastres naturales como incendios o corto circuitos, etc. con el cual se evitaría que el trabajo sea interrumpido y se daría continuidad inmediata al negocio.

Capítulo 3

Levantamiento de activos de la Información

3.1 Levantamiento de activos de información

Luego de haber realizado la respectiva investigación en el hospital y haber observado el funcionamiento, se procedió a realizar el levantamiento de activos y el análisis de todos los puntos tratados anteriormente, tanto en hardware, software, recursos humanos, servicios, edificación y redes de comunicación. Para realizar el levantamiento se realizó una entrevista a los usuarios donde se les preguntaba acerca de la información que manejan y como la manejan y además el método de observación acerca de la edificación, del manejo de la información en papel, de los controles de acceso a las áreas restringidas, etc. Y luego con la información recolectada se procedió a elaborar las matrices según Magerit.

3.1.1 Activos Hardware

Como hardware se señalan todos los equipos informáticos físicos que concentran y almacenan información que está destinada a soportar los servicios que presta la empresa. Para la matriz de los activos de información de hardware del Hospital Santa Inés se han planteado los siguientes campos:

a. **ID HARD:** que representa el código del activo de hardware, el cual según Magerit está representado por [HARDWARE][TIPO DE HARDWARE]NUMERO, donde tipo de hardware tiene varios equipos que son:
    a. [host] grandes equipos
    b. [mid] equipos medios
    c. [pc] informática personal
    d. [mobile] informática móvil
    e. [pda] agendas electrónicas
    f. [easy] fácilmente remplazable
    g. [data] que almacena datos
    h. [peripheral] periféricos
        i. [print] medios de impresión
        ii. [scan] scanner

iii. [crypto] dispositivos criptográficos

i. [network] soporte a la red
    i. [modem] módems
    ii. [hub] concentradores
    iii. [switch] conmutadores
    iv. [router] encaminadores
    v. [bridge] pasarelas
    vi. [firewall] cortafuegos
    vii. [wap] punto de acceso wireless

j. [pabx] centralita telefónica

Un ejemplo es [HW][PC]1 o [HW][NETWORK][FIREWALL]1

b. **ID RRHH:** Hace referencia al código de empleado. Consiste en un campo que se encuentra en la matriz de recursos humanos en donde se encuentran todos los empleados del Hospital, el cual según Magerit está representado por [PERSONAL][TIPO DE PERSONAL]NUMERO, donde tipo de personal puede ser:
    a. [ue] usuarios externos
    b. [ui] usuarios internos
    c. [op] operadores
    d. [adm] administradores de sistemas
    e. [com] administradores de comunicaciones
    f. [dba] administradores de BBDD
    g. [des] desarrolladores
    h. [sub] subcontratas
    i. [prov] proveedores

    Un ejemplo es [P][UI]1 o [P][ADM]11

c. **Empleado:** este campo corresponde al nombre del empleado que maneja el equipo.

d. **Tipo de activo:** puede ser
    a. [host] grandes equipos
    b. [mid] equipos medios
    c. [pc] informática personal
    d. [mobile] informática móvil
    e. [pda] agendas electrónicas
    f. [easy] fácilmente remplazable
    g. [data] que almacena datos
    h. [peripheral] periféricos
        i. [print] medios de impresión
        ii. [scan] scanner
        iii. [crypto] dispositivos criptográficos
    i. [network] soporte a la red
        i. [modem] módems
        ii. [hub] concentradores
        iii. [switch] conmutadores
        iv. [router] encaminadores
        v. [bridge] pasarelas
        vi. [firewall] cortafuegos
        vii. [wap] punto de acceso wireless
    j. [pabx] centralita telefónica

e. **Nombre Equipo:** es el nombre registrado de cada equipo.
f. **Dirección MAC:** es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red
g. **IP:** cada dispositivo conectado a una red se le asigna un número único conocido como dirección de Internet Protocolo (IP). Estas direcciones consisten en cuatro números separados por puntos y parecen algo como 127.0.0.1.
h. Confidencialidad: para analizar este punto utilice la siguiente escala:

Escala	Valor
Publico: acceso libre (incluso pacientes)	1
Interno: solo personal del hospital	2
Confidencial: solo el departamento al que corresponde	3

i. **Disponibilidad:** utilice la siguiente escala

Escala	Valor
Puede permanecer sin información de 8 a 120 horas	1
Puede permanecer sin información de 2 a 8 horas	2
Puede permanecer sin información de 1 a 2 horas	3

j. **Integridad**

Escala	Valor
La información debe tener un 90% de exactitud	1
La información debe tener un 97% de exactitud	2
La información debe tener un 100% de exactitud	3

3.1.2 Activos Software

Como software se enmarcan los programas y las aplicaciones que se desempeñan en los computadores, que son los que transforman los datos en información. Para la matriz de los activos de información de software del Hospital Santa Inés se utilizaron los siguientes campos:

a. **ID SOFT:** que representa el código del activo de software, el cual según Magerit está representado por [SOFTWARE][TIPO DE SOFTWARE]NUMERO, donde tipo de software tiene varios equipos que son:
    a. [prp] desarrollo propio
    b. [sub] desarrollo a medida
    c. [std] estándar
        i. [browser] navegador web
        ii. [www] servidor de presentación
        iii. [app] servidor de aplicaciones
        iv. [email_client] cliente de correo electrónico
        v. [file] servidor de ficheros
        vi. [dbms] sistema de gestión de base de datos
        vii. [tm] monitor transaccional
        viii. [office] ofimática
        ix. [av] antivirus
        x. [os] sistema operativo
        xi. [ts] servidor de terminales
        xii. [backup sistema de backup]

    Un ejemplo es [SW][OFFICE]1

b. **ID RRHH:** este es el código de empleado es un campo que se encuentra en la matriz de Recursos Humanos en donde se encuentran todos los empleados del Hospital, el cual según Magerit está representado por [PERSONAL][TIPO DE PERSONAL]NUMERO, donde tipo de personal puede ser:
    a. [ue] usuarios externos
    b. [ui] usuarios internos
    c. [op] operadores
    d. [adm] administradores de sistemas

e. [com] administradores de comunicaciones
f. [dba] administradores de BBDD
g. [des] desarrolladores
h. [sub] subcontratas
i. [prov] proveedores

Un ejemplo es [P][UI]1 o [P][ADM]11

c. **Empleado:** este campo corresponde al nombre del empleado que maneja el equipo.
d. **Nombre Equipo:** es el nombre registrado de cada equipo.
e. **Tipo de software:** puede ser
    a. [prp] desarrollo propio
    b. [sub] desarrollo a medida
    c. [std] estándar
        i. [browser] navegador web
        ii. [www] servidor de presentación
        iii. [app] servidor de aplicaciones
        iv. [email_client] cliente de correo electrónico
        v. [file] servidor de ficheros
        vi. [dbms] sistema de gestión de base de datos
        vii. [tm] monitor transaccional
        viii. [office] ofimática
        ix. [av] antivirus
        x. [os] sistema operativo
        xi. [ts] servidor de terminales
        xii. [backup sistema de backup]

f. **Software:** va el nombre de software del equipo.
g. **Licencia:** número de la licencia del programa de cada computadora
h. **Procesos:** los procesos de la clínica que se realiza cada usuario.

3.1.3 Activos de Edificación

La edificación representa las instalaciones del Hospital, la ubicación de sus departamentos. Para esta matriz se utilizaron los siguientes campos:

a. **ID EDIFICACION:** que representa el código del activo de edificación, el cual según Magerit está representado por [INSTALACIONES][TIPO DE INSTALACION][PISO]NUMERO, donde tipo de instalación tiene varios equipos que son:
    a. [site] emplazamiento
    b. [building] edificio
    c. [local] local
    d. [mobile] plataformas móviles
        i. [car] vehículo terrestre: coche, camión, etc.
        ii. [plane] vehículo aéreo: avión, etc.
        iii. [ship] vehículo marítimo: buque, lancha, etc.
        iv. [shelter] contenedores
    e. [cannel] canalizadores

    Un ejemplo es [L][BUILDING][PISO5]1

b. **ID RRHH:** este es el código de empleado es un campo que se encuentra en la matriz de recursos humanos en donde se encuentran todos los empleados del Hospital, el cual según magerit está representado por [PERSONAL][TIPO DE PERSONAL]NUMERO, donde tipo de personal puede ser:
    a. [ue] usuarios externos
    b. [ui] usuarios internos
    c. [op] operadores
    d. [adm] administradores de sistemas
    e. [com] administradores de comunicaciones
    f. [dba] administradores de BBDD

g. [des] desarrolladores
h. [sub] subcontratas
i. [prov] proveedores

Un ejemplo es [P][UI]1 o [P][ADM]11

c. **Empleado:** este campo corresponde al nombre del empleado que maneja el equipo.
d. **Nombre Equipo:** es el nombre registrado de cada equipo.
e. **Departamento:** en este campo va el nombre de cada departamento donde se encuentra el activo
f. **Planta:** es el número de piso en el que se encuentra el departamento, va del 1-5.
g. Confidencialidad: para analizar este punto utilice la siguiente escala:

Escala	Valor
Publico: acceso libre (incluso pacientes)	1
Interno: solo personal del hospital	2
Confidencial: solo el departamento al que corresponde	3

h. Disponibilidad: utilice la siguiente escala

Escala	Valor
Puede permanecer sin información de 8 a 120 horas	1
Puede permanecer sin información de 2 a 8 horas	2
Puede permanecer sin información de 1 a 2 horas	3

i. Integridad

Escala	Valor
La información debe tener un 90% de exactitud	1
La información debe tener un 97% de exactitud	2
La información debe tener un 100% de exactitud	3

3.1.4 Activos de equipo auxiliar

El equipo auxiliar otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con los datos como son los UPS, los generadores eléctricos, etc. para la matriz de los activos se utilizó los siguientes campos:

- **a. ID:** el código del equipo auxiliar según Magerit está representado por [AUXILIAR][TIPO DE EQUIPO]NUMERO, donde el tipo de equipo puede ser:
  - **a.** [power]fuentes de alimentación
  - **b.** [ups] sistemas de alimentación interrumpida
  - **c.** [gen] generadores eléctrico
  - **d.** [ac] equipos de climatización
  - **e.** [cabling] cableado
  - **f.** [robot] robots
    - **i.** [tape] … de cintas
    - **ii.** [disk] … de discos
  - **g.** [supply] suministros esenciales
  - **h.** [destroy] equipos de destrucción de soportes de información
  - **i.** [furniture] mobiliario: armarios, etc.
  - **j.** [safe] cajas fuertes
- **b. Descripción:** en este campo va el nombre del equipo auxiliar como por ejemplo los UPS, el generador eléctrico, etc.

c. **Fecha de instalación:** es la fecha en la que lo instalaron en el hospital
d. **Estado:** fueron analizados según como se encontraban físicamente, donde bueno significa que su estado es el mejor, que no ha sufrido ningún daño
e. **Observaciones:** en el caso de que algún equipo requiera una observación especial
f. **Ubicación:** con la matriz de edificación se llena con el código de la edificación según el piso en donde se encuentre el equipo

3.1.5 Activos de Recursos Humanos

Dentro de los recursos humanos se encuentra el personal del hospital y los campos que se utilizaron son los siguientes campos:

a. **ID RRHH**: el código del empleado es un campo que se encuentra en la matriz de recursos humanos en donde se contemplan todos los empleados del Hospital, el cual según Magerit, está representado por [PERSONAL][TIPO DE PERSONAL]NUMERO, donde tipo de personal puede ser:
    a. [ue] usuarios externos
    b. [ui] usuarios internos
    c. [op] operadores
    d. [adm] administradores de sistemas
    e. [com] administradores de comunicaciones
    f. [dba] administradores de BBDD
    g. [des] desarrolladores
    h. [sub] subcontratas
    i. [prov] proveedores

    Un ejemplo es [P][OP]

b. **Empleado:** el nombre de los empleados del Hospital Santa Inés

c. **Tipo de activo**: que puede ser
    a. [ue] usuarios externos
    b. [ui] usuarios internos
    c. [op] operadores
    d. [adm] administradores de sistemas
    e. [com] administradores de comunicaciones
    f. [dba] administradores de BBDD
    g. [des] desarrolladores
    h. [sub] subcontratas
    i. [prov] proveedores

3.1.6 Activos de Soporte de la Información

Dentro de los sopores de información se consideran dispositivos físicos para almacenar información de forma permanente. Para la matriz de los activos de soportes de información los siguientes campos:

a. ID: el código del equipo soporte según Magerit está representado por [SOPORTE][TIPO DE EQUIPO]NUMERO, donde el tipo de equipo puede ser:
    a. [electronic] electrónicos
        i. [discos] discos
        ii. [san] almacenamiento de red
        iii. [disquette] disquetes
        iv. [cd] CD-ROM
        v. [usb] dispositivo USB
        vi. [dvd] DVD
        vii. [tape] cinta magnética
        viii. [mc] tarjetas de memoria
        ix. [ic] tarjetas inteligentes
    b. [non_electronic] no electrónicos
        i. [printed] material impreso

ii. [tapet] cinta de papel
iii. [film] microfilm
iv. [cards] tarjetas perforadas

b. **Descripción:** en este campo va el nombre del soporte.
c. **ID RRHH:** este campo corresponde a la matriz de Recursos Humanos
d. **Empleado:** es el nombre del empleado a quien le corresponde el soporte
e. **Estado:** fueron analizados según como se encontraban físicamente, donde bueno significa que su estado es el mejor, que no ha sufrido ningún daño
f. **Ubicación:** corresponde a la matriz de edificación según el departamento en donde se encuentre.
g. **Confidencialidad:** para analizar este punto utilice la siguiente escala:

Escala	Valor
Publico: acceso libre (incluso pacientes)	1
Interno: solo personal del hospital	2
Confidencial: solo el departamento al que corresponde	3

h. **Disponibilidad:** utilice la siguiente escala

Escala	Valor
Puede permanecer sin información de 8 a 120 horas	1
Puede permanecer sin información de 2 a 8 horas	2
Puede permanecer sin información de 1 a 2 horas	3

i. Integridad

Escala	Valor
La información debe tener un 90% de exactitud	1
La información debe tener un 97% de exactitud	2
La información debe tener un 100% de exactitud	3

3.1.7 Activos de Servicios

Los servicios son todos aquellos que se les presta a los usuarios dentro del hospital para que su desempeño sea optimo, los servicios pueden ser finales (prestados por la Organización a terceros), instrumentales (donde tanto los usuarios como los medios son propios) o bien contratados (a otra organización que los proporciona).

a. ID: el código del servicio según Magerit está representado por [SERVICIO][TIPO DE SERVICIO]NUMERO, donde el tipo de servicio puede ser:

- **a.** [anon]anónimo (sin requerir identificación del usuario)
- **b.** [pub] público en general (sin relación contractual)
- **c.** [ext] a usuarios externos (bajo una relación contractual)
- **d.** [int] interno (usuarios y medios de la propia organización)
- **e.** [cont] contratado a terceros
- **f.** [www] world wide web
- **g.** [telnet] acceso remoto a cuenta local
- **h.** [email] correo electrónico
- **i.** [file] almacenamiento de ficheros
- **j.** [ftp] transferencia de ficheros
- **k.** [edi] intercambio electrónico de datos

l. [dis] servicio de directorio
m. [idm] gestión de identidades
n. [ipm] gestión de privilegios
o. [pki] PKI – infraestructura de clave publica

b. **Descripción:** este campo corresponde al nombre del servicio como por ejemplo internet, correo electrónico.
c. **Fecha de instalación:** es la fecha en la que lo instalaron en el hospital
d. **Estado:** activo – desactivo , según como se encontró actualmente
e. **Observaciones:** en el caso de que algún equipo requiera una observación especial
f. **Ubicación:** con la matriz de edificación se llena con el código de la edificación según el piso en donde se encuentre el equipo

3.1.8 Activos de las redes de comunicación

Las redes de comunicación son las instalaciones dedicadas así como servicios de comunicación contratados a terceros, pero son los medios que llevan datos de un lado a otro.

a. **ID:** el código de la red según Magerit está representado por [COM:RED DE COMUNICION][TIPO DE RED]NUMERO, donde el tipo de red puede ser:
   a. [pstn] red telefónica
   b. [isdn] rdsi (red digital)
   c. [x25] x25 (red de datos)
   d. [adsl] ADSL
   e. [pp] punto a punto
   f. [radio] red inalámbrica
   g. [sat] por satélite
   h. [LAN] red local

i. [man] red metropolitana
j. [internet] internet
k. [vpn] red privada virtual

b. **Descripción:** este campo corresponde al nombre de la red
c. **Fecha de instalación:** es la fecha en la que lo instalaron en el hospital
d. **Estado:** activo – desactivo , según como se encontró actualmente
e. **Observaciones:** en el caso de que algún equipo requiera una observación especial
f. **Ubicación:** con la matriz de edificación se llena con el código de la edificación según el piso en donde se encuentre el equipo

3.2 Identificación de procesos del negocio

Para la identificación de procesos se realizó un análisis de todas las actividades que se realizan en cada departamento del hospital, ya que las organizaciones se basan en desarrollar actividades, las cuales se agrupan para dar procesos. Para realizar este análisis el hospital colaboró con un archivo con los subprocesos previamente elaborado, de donde se obtuvieron los procesos principales. Anexo 4

3.3 Clasificación de niveles de confidencialidad de cada activo

Para la clasificación de los niveles de confidencialidad se utilizó el dimensionamiento de valoración según Magerit, donde se analiza la importancia que tendría que un dato fuera conocido por personas no autorizadas, donde los datos reciben el valor más alto si su revelación provocaría graves daños a la organización y de lo contrario reciben un valor mínimo si su conocimiento por cualquier persona no provocaría ningún daño. La escala fue la siguiente:

Escala	Valor
Publico: acceso libre (incluso pacientes)	1
Interno: solo personal del hospital	2
Confidencial: solo el departamento al que corresponde	3

3.4 Clasificación de la disponibilidad de la información

Para la clasificación de los niveles de confidencialidad se utilizó el dimensionamiento de valoración según Magerit, donde se analiza la importancia que tendría que un activo no estuviera disponible, donde el valor más alto se da cuando un activo no puede estar por mucho tiempo indisponible y de lo contrario reciben un valor mínimo el activo podría estar durante periodos largos indisponible sin causar daño. La escala fue la siguiente:

Escala	Valor
Puede permanecer sin información de 8 a 120 horas	1
Puede permanecer sin información de 2 a 8 horas	2
Puede permanecer sin información de 1 a 2 horas	3

3.5 Clasificación por niveles de los activos

La clasificación por niveles de los activos se realizó según Magerit, donde se organiza jerárquicamente, según el tipo de activo se va codificando cada elemento. Los tipos de activos son:

- [S] Servicio
- [D] Datos / Información
- [SW] Aplicaciones (software)
- [HW] Equipos informáticos (hardware)
- [COM] Redes de comunicación
- [SI] Soportes de información
- [AUX] Equipamiento auxiliar
- [L] Instalaciones
- [P] Personal

Y según esta clasificación de los activos se elaboraron las matrices respectivas

3.6 Identificación de las amenazas, riesgos y probabilidades de impacto

La identificación de amenazas y riesgos es el paso final antes de realizar las Políticas de Seguridad de la Información, aquí se debe tomar en cuenta todas las amenazas que podrían poner en riesgo los activos de la información ya sean por irresponsabilidad de los operadores, desastres naturales, fallas en el software o hardware, etc. Luego de identificar las amenazas y riegos se procede a analizar la probabilidad de impacto, que es la posibilidad de que estos eventos ocurran, por ejemplo la probabilidad de que haya una inundación por una gotera es baja, pero la probabilidad de que se dañen los discos duros por el paso del tiempo es alta. La escala que se utilizó para la probabilidad de ocurrencia es alto, medio y bajo.

Las amenazas que se identificaron fueron:

AMENAZA	RIESGO O TRETA
N.1 [FUEGO]	CORTOCIRCUITO
	COCINA
	EXPLOSION BOTELLON GAS
	RAYO
N.2 [INUNDACION]	CAÑERIA ROTA
	GOTERAS
	UNA LLAVE ABIERTA

AMENAZA	RIESGO O TRETA
N.3 [TERREMOTO]	DESASTRE NATURAL
I.1 [CONTAMINACION MECANICA]	POLVO
	SUCIEDAD
	COMER SOBRE EQUIPOS
	DERRAMAR LIQUIDOS SOBRE EQUIPOS
I.2 [CONTAMINACION ELECTROMAGNETICA]	INTERFERENCIA DE RADIO
	CAMPOS MAGNETICOS
I.3 [FALLOS FISICOS O LOGICOS]	FALLOS
I.4 [SUMINISTRO ELECTRICO]	CORTE ELECTRICIDAD
	SOBRECARGA ELECTRICA
I.5 [INTERRUPCION DE OTROS SERVICIOS Y SUMINISTRSO]	TERMINE PAPEL IMPRESORA
	TERMINE EL TONER
I.6 [DEGRADACION EQUIPOS ALMACENAMIENTO]	SE DAÑEN LOS DISCOS DUROS POR PASO DEL TIEMPO
	SE DAÑEN POR MAL USO
E.1 [FALLOS NO INTENCIONADOS]	EQUIVOCACION DE USUARIOS AL INGRESAR INFORMACION DE PACIENTES
	PÉRDIDA ACCIDENTAL DE LA INFORMACION
	REVELACON DE INFORMACION POR INDISCRECION
	EQUIVOCACION DE ADMINISTRADOR EN INSTALACIONES
	FALTA EN LOS REGISTROS
	SOFTWARE DAÑINO (VIRUS, SPYWARE, TROYANOS)
	ERRORES EN EL MANTENIMIENTO DE SOFTWARE
	ERRORES EN EL MANTENIMIENTO DE HARDWARE
	AUSENCIA EN EL PUESTO DE TRABAJO
A.2 [FALLOS INTENCIONADOS]	MANIPUACION EN LA CONFIGURACION
	SUPLANTACION DE LA IDENTIDAD DE UN USUARIO
	ABUSO DE PRIVILEGIOS OTROGADOS

AMENAZA	RIESGO O TRETA
A.2 [FALLOS INTENCIONADOS]	USO DE LOS EQUIPOS PARA COSAS PERSONALES (INTERNET, GUARDAR INFORMACION PERSONAL)
	ALTERACION ORDEN PAQUETES TRANSMITIDOS
	ANALISIS DEL TRANSITO
	MODIFICACION DE LA INFORMACION
	INTRODUCCION INFORMACION FALSA
	ROBO DE LOS EQUIPOS
	ATAQUE DESTRUCTIVO (VANDALISMO)

Capítulo 4

Elaboración de las Políticas de Seguridad de la Información

Aquí se presentan las Políticas de Seguridad de la Información donde según las amenazas que podrían afectar la disponibilidad, integridad y confidencialidad de los activos de la información del Hospital Santa Inés, y cada una de las actividades que se debe tener en cuenta para evitar que la amenaza se cumpla. Algunas de estas actividades cuentan con cuadros de referencia que se adjuntaron al archivo.

4.1 Políticas de Edificación

EDIFICACIÓN			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de las instalaciones del centro de procesamiento de datos	Sobre instalación y control de los elementos físicos del centro de cómputo	Incendio	1) El centro de cómputo debe estar ubicado en un lugar que no contenga material inflamable, y tampoco situarse cerca de áreas donde se almacenen materiales inflamables (REF. MAT-INF) 2) Prohibido fumar en el área de cómputo 3) El centro de cómputo debe tener muebles no combustibles y la mayor parte de productos de oficina metálicos 4) Los extintores son una parte fundamental se debe adquirir y ubicarlos en lugares estratégicos además de capacitar al personal 5) Para el cuarto de servidores se deberá adquirir extintores con componente de soda-ácido, para que los equipos informáticos no sufran daños. 6) Se debe instalar, un sistema de alarmas y detectores de humo. 7) Instalar un sistema automático contra incendios a base de gas, por lo que es fundamental que el cuarto este bien cerrado sin escape de aire.
	Sobre mantenimiento de los equipos contra incendios del centro de cómputo		1) Los extintores no deben estar bloqueados por equipos, abrigos u otros objetos que puedan interferir con el acceso en caso de emergencia. 2) Revisar que los extintores no tengan abolladuras, fugas óxido, depósitos de productos químicos. 3) Algunos fabricantes recomiendan sacudir el extintor una vez al mes. 4) Semestralmente se debe comunicar con los bomberos para que realicen un mantenimiento de los extintores, alarmas y detectores de humo.

EDIFICACIÓN			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de las instalaciones del centro de procesamiento de datos	Sobre instalación y control del cableado del centro de cómputo	Evento de cortocircuito	1) El hospital debe contratar a una empresa calificada para que certifique y documente de una manera detallada el cableado estructurado, cumpliendo con las normas y estándares internacionales establecidos.
	Sobre mantenimiento del cableado del centro de cómputo		1) Realizar una revisión trimestral de las condiciones del cableado eléctrico y acometidas 2) Reportar la revisión en un formato de informe al departamento de sistemas
	Sobre instalación y control de las tuberías del centro de cómputo	Evento de gotera e inundación	1) El centro de cómputo debe mantenerse en un lugar alejado de baños, tuberías y otras fuentes de agua.
	Sobre mantenimiento de tuberías del centro de cómputo		1) Revisar que las vías y conductos de ventilación no puedan ser afectados por lluvia, o agua producida por un generador de aire acondicionado. 2) Revisión trimestral de los tuberías de agua basándose en la plantilla EDI-CPD-EDG-001 3) Reportar la revisión en un formato de informe al departamento de sistemas basado en la plantilla EDI-CPD-EGD-001
	Sobre el control de las instalaciones del centro de cómputo	Terremoto	1) Fijar los muebles del hospital para que en caso de un terremoto no se muevan 2) Colocar una película o film en los cristales para que si se rompen no salgan despedidos por el lugar 3) Asegurarse de que los respaldos de información se encuentren en un lugar seguro fuera de un rango de 3 km a la redonda.

EDIFICACIÓN			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de las instalaciones del centro de procesamiento de datos	Sobre el mantenimiento de las instalaciones del centro de cómputo		1) Realizar un diagnóstico sobre la resistencia de la construcción 2) En caso de ser necesario mejorar la resistencia
	Sobre prevención de un corte eléctrico en el centro de cómputo	Evento de corte eléctrico	1) Los servidores y computadores del centro de cómputo deben contar con UPS (Uninterruptible Power Supply) para permitir el apagado correcto de los mismos. 2) El Hospital Santa Inés debe tener un generador privado para casos de cortes eléctricos 3) La planta de energía eléctrica debe encenderse automáticamente cuando se presente el apagón.
	Sobre mantenimiento de generador eléctrico para el centro de cómputo		1) Se debe realizar un mantenimiento del generador cada tres meses para asegurarse de que funciona 2)Los UPS deben ser revisados cada 3 meses 3) Reportar la revisión
	Sobre control eléctrico del centro de cómputo	Evento de sobrecarga eléctrica	1) Asegúrese de que los equipos estén conectados a tierra, verificando que en una prueba utilizando el multímetro, el neutro con la fase debe dar menos de 10A 2) Mensualmente se debe supervisar las líneas eléctricas en busca de ruido 3) Registrar las evaluaciones y sus resultados en la bitácora EDI-CPD-SEL-001

EDIFICACIÓN			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de las instalaciones del quirófano	Sobre instalación y control de los elementos físicos del quirófano	Incendio	1) El quirófano no debe contener material inflamable, ni debe situarse cerca de áreas donde se almacenen materiales inflamables 2) Prohibido fumar en el quirófano 3) El quirófano debe tener muebles no combustibles 4) Los extintores son una parte fundamental se debe adquirir y ubicarlos en lugares estratégicos además de capacitar al personal 5) Se debe instalar, un sistema de alarmas y detectores de humo. 6) Instalar un sistema automático contra incendios a base de gas, por lo que es fundamental que el cuarto este bien cerrado sin escape de aire.
	Sobre mantenimiento de los equipos contra incendios del quirófano		1) El extintor no debe estar bloqueado por equipos, abrigos u otros objetos que puedan interferir con el acceso en caso de emergencia. 2) Revisar que el extintor no tenga abolladuras, fugas óxido, depósitos de productos químicos. 3) Algunos fabricantes recomiendan sacudir el extintor una vez al mes. 4) Semestralmente se debe comunicar con los bomberos para que realicen un mantenimiento de los extintores, alarmas y detectores de humo.
	Sobre instalación y control del cableado del quirófano	Evento de cortocircuito	1) El hospital debe contratar a una empresa calificada para que certifique y documente de una manera detallada el cableado estructurado, para que se cumpla con las normas y estándares establecidos.

EDIFICACIÓN			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de las instalaciones del quirófano	Sobre mantenimiento del cableado del quirófano		1) Realizar una revisión trimestral de las condiciones del cableado eléctrico y acometidas basándose en la plantilla EDI-CPD-ELEC-001 3) Reportar la revisión en un formato de informe al departamento de sistemas
	Sobre instalación y control de las tuberías del quirófano	Evento de gotera e inundación	1) El quirófano debe mantenerse en un lugar alejado de baños, tuberías y otras fuentes de agua.
	Sobre mantenimiento de tuberías del quirófano		1) Revisar que las vías y conductos de ventilación no puedan ser afectados por lluvia, o agua producida por un generador de aire acondicionado. 2 Revisión trimestral de los tuberías de agua basándose en la plantilla EDI-CPD-EDG-001 3) Reportar la revisión en un formato de informe al departamento de sistemas basado en la plantilla EDI-CPD-EGD-001
	Sobre instalación y control de las tuberías del quirófano	Terremoto	1) Fijar los muebles del hospital para que en caso de un terremoto no se muevan 2) Colocar una película o film en los cristales para que si se rompen no salgan despedidos por el lugar 3) Asegurarse de que los respaldos de información se encuentren en un lugar seguro fuera de un rango de 3 km a la redonda.
	Sobre mantenimiento de tuberías del quirófano		1) Realizar un diagnóstico sobre la resistencia de la construcción 2) En caso de ser necesario mejorar la resistencia

EDIFICACIÓN			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de las instalaciones del quirófano	Sobre prevención de un corte eléctrico en el quirófano	Evento de corte eléctrico	1) Los equipos informáticos del quirófano deben contar con UPS para permitir el apagado correcto de los mismos.
	Sobre mantenimiento de generador eléctrico para el quirófano		1) Se debe realizar un mantenimiento del generador cada tres meses para asegurarse de que funciona 2) Los UPS deben ser revisados cada 3 meses
	Sobre control eléctrico del quirófano	Evento de sobrecarga eléctrica	1) Asegúrese de que los equipos estén conectados a tierra, verificando que en una prueba utilizando el multímetro, el neutro con la fase debe dar menos de 10A 2) Mensualmente se debe supervisar las líneas eléctricas en busca de ruido 3) Registrar las evaluaciones y sus resultados en la bitácora EDI-CPD-SEL-001.
Sobre el control de las instalaciones de UCI	Sobre instalación y control de los elementos físicos de emergencia	Incendio	1) Emergencia no debe contener material inflamable, ni debe situarse cerca de áreas donde se almacenen materiales inflamables 2) Prohibido fumar en el quirófano 3) Emergencia debe tener muebles no combustibles 4) Los extintores son una parte fundamental se debe adquirir y ubicarlos en lugares estratégicos además de capacitar al personal 5) Se debe instalar, un sistema de alarmas y detectores de humo. 6) Instalar un sistema automático contra incendios a base de gas, por lo que es fundamental que el cuarto este bien cerrado sin escape de aire.

EDIFICACIÓN			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de las instalaciones de UCI	Sobre mantenimiento de los equipos contra incendios de emergencia	Incendio	1) El extintor no debe estar bloqueado por equipos, abrigos u otros objetos que puedan interferir con el acceso en caso de emergencia. 2) Revisar que el extintor no tenga abolladuras, fugas óxido, depósitos de productos químicos. 3) Algunos fabricantes recomiendan sacudir el extintor una vez al mes. 4) Semestralmente se debe comunicar con los bomberos para que realicen un mantenimiento de los extintores, alarmas y detectores de humo.
	Sobre instalación y control del cableado de emergencia	Evento de cortocircuito	1) El hospital debe contratar a una empresa calificada para que certifique y documente de una manera detallada el cableado estructurado, para que se cumpla con las normas y estándares establecidos.
	Sobre mantenimiento del cableado de emergencia		1) Realizar una revisión trimestral de las condiciones del cableado eléctrico y acometidas basándose en la plantilla EDI-CPD-ELEC-001 3) Reportar la revisión en un formato de informe al departamento de sistemas
	Sobre instalación y control de las tuberías de emergencia	Evento de gotera e inundación	1) El quirófano debe mantenerse en un lugar alejado de baños, tuberías y otras fuentes de agua.

EDIFICACIÓN			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de las instalaciones de UCI	Sobre mantenimiento de tuberías de emergencia	Evento de gotera e inundación	1) Revisar que las vías y conductos de ventilación no puedan ser afectados por lluvia, o agua producida por un generador de aire acondicionado. 2) Revisión trimestral de los tuberías de agua basándose en la plantilla EDI-CPD-EDG-001 3) Reportar la revisión en un formato de informe al departamento de sistemas basado en la plantilla EDI-CPD-EGD-001
	Sobre instalación y control de las tuberías de emergencia	Terremoto	1) Fijar los muebles del hospital para que en caso de un terremoto no se muevan. 2) Colocar una película o film en los cristales para que si se rompen no salgan despedidos por el lugar. 3) Asegurarse de que los respaldos de información se encuentren en un lugar seguro fuera de un rango de 3 km a la redonda.
	Sobre mantenimiento de tuberías de emergencia		1) Realizar un diagnóstico sobre la resistencia de la construcción. 2) En caso de ser necesario mejorar la resistencia.
	Sobre prevención de un corte eléctrico de emergencia	Evento de corte eléctrico	1) Los equipos informáticos del quirófano deben contar con UPS para permitir el apagado correcto de los mismos.
	Sobre mantenimiento de generador eléctrico para de emergencia		1) Se debe realizar un mantenimiento del generador cada tres meses para asegurarse de que funciona. 2) los UPS deben ser revisados cada 3 meses.

EDIFICACIÓN			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de las instalaciones de UCI	Sobre control eléctrico de emergencia	Evento de sobrecarga eléctrica	1) Asegúrese de que los equipos estén conectados a tierra, verificando que en una prueba utilizando el multímetro, el neutro con la fase debe dar menos de 10A. 2) Mensualmente se debe supervisar las líneas eléctricas en busca de ruido. 3) Registrar las evaluaciones y sus resultados en la bitácora EDI-CPD-SEL-001.
Sobre el control de las instalaciones en general	Sobre instalación y control de los elementos físicos	Incendio	1) Las instalaciones no deben contener material inflamable, ni debe situarse cerca de áreas donde se almacenen materiales inflamables. 2) Prohibido fumar en las instalaciones. 3) Las instalaciones deben tener muebles no combustibles. 4) Los extintores son una parte fundamental se debe adquirir y ubicarlos en lugares estratégicos además de capacitar al personal. 5) Se debe instalar, un sistema de alarmas y detectores de humo. 6) Instalar un sistema automático contra incendios a base de gas, por lo que es fundamental que el cuarto este bien cerrado sin escape de aire.
	Sobre mantenimiento de los equipos contra incendios		1) El extintor no debe estar bloqueado por equipos, abrigos u otros objetos que puedan interferir con el acceso en caso de emergencia. 2) Revisar que el extintor no tenga abolladuras, fugas óxido, depósitos de productos químicos. 3) Algunos fabricantes recomiendan sacudir el extintor una vez al mes. 4) Semestralmente se debe comunicar con los bomberos para que realicen un mantenimiento de los extintores, alarmas y detectores de humo.

EDIFICACIÓN			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de las instalaciones en general	Sobre instalación y control del cableado	Evento de cortocircuito	1) El hospital debe contratar a una empresa calificada para que certifique y documente de una manera detallada el cableado estructurado, para que se cumpla con las normas y estándares establecidos.
	Sobre mantenimiento de tuberías	Evento de gotera e inundación	1) Revisar que las vías y conductos de ventilación no puedan ser afectados por lluvia, o agua producida por un generador de aire acondicionado. 2) Revisión trimestral de los tuberías de agua basándose en la plantilla EDI-CPD-EDG-001 3) Reportar la revisión en un formato de informe al departamento de sistemas basado en la plantilla EDI-CPD-EGD-001
	Sobre instalación y control de las tuberías	Terremoto	1) Fijar los muebles del hospital para que en caso de un terremoto no se muevan 2) Colocar una película o film en los cristales para que si se rompen no salgan despedidos por el lugar 3) Asegurarse de que los respaldos de información se encuentren en un lugar seguro fuera de un rango de 3 km a la redonda.
	Sobre mantenimiento de tuberías		1) Realizar un diagnóstico sobre la resistencia de la construcción 2) En caso de ser necesario mejorar la resistencia

EDIFICACIÓN			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de las instalaciones en general	Sobre prevención de un corte eléctrico	Evento de corte eléctrico	1) Los computadores y maquinas del quirófano deben contar con UPS para permitir el apagado correcto de los mismos.
	Sobre mantenimiento de generador eléctrico para		1) Se debe realizar un mantenimiento del generador cada tres meses para asegurarse de que funciona 2) los UPS deben ser revisados cada 3 meses
	Sobre control eléctrico	Evento de sobrecarga eléctrica	1) Asegúrese de que los equipos estén conectados a tierra, verificando que en una prueba utilizando el multímetro, el neutro con la fase debe dar menos de 10A 2) Mensualmente se debe supervisar las líneas eléctricas en busca de ruido 3) Registrar las evaluaciones y sus resultados en la bitácora EDI-CPD-SEL-001
Sobre el control de acceso a las instalaciones del centro de cómputo	Sobre las instalaciones para control de acceso al centro de cómputo	Robo o daño de la información	1) El centro de cómputo debe permanecer cerrado con llave. 2) Además el centro de cómputo debe tener una cerradura de acceso biométrico. 3) Al ingresar al centro de cómputo la persona debe registrarse obligatoriamente (ref. PCA-PIC-001).
	Sobre el control de acceso de personal al centro de cómputo		1) Cualquier persona no autorizado al centro de cómputo debe solicitar con anticipación la visita. 2) Además se debe realizar un comunicado interno firmado y autorizado por el jefe inmediato 3) Una vez concedido el permiso deberá registrarse (ref. PCA-PIC-001)

EDIFICACIÓN			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de acceso a las áreas restringidas del Hospital Santa Inés	Sobre el registro para ingreso a áreas restringidas	Suplantación de la identidad de un usuario	1) Pedir autorización al jefe del departamento. 2) Llenar solicitud de ingreso temporal (PCA-PIC-001). 3) Se llevará un registro permanente del tráfico de personal, sin excepción.
Sobre la señalización del hospital	Sobre la instalación de las señales para emergencias en el hospital	Desastres naturales	1) La altura para colocar las señales es de 1.80 metros a 2.1 metros medidos desde el piso. 2) Las señales de salida de emergencia se colocaran en la parte superior del marco de la puerta de evacuación. 3) La señal de extintor se colocara a una altura de 1.80 metros y el equipo a 1.50 metros.
	Sobre el mantenimiento de la señalización del Hospital		1) No se debe colocar ningún otro aviso cerca de la señal de seguridad ya que puede impedir la visibilidad. 2) Se debe mantener libre el espacio donde este colocado el extintor. 3) Revisar la fecha de caducidad de los equipos para recargarlos inmediatamente 4) las señales foto luminosas son importantes para indicar las rutas de evacuación. 5) Se debe dar capacitaciones al personal para que todos sepan cómo actuar.

4.2 Políticas de Recursos Humanos

RECURSOS HUMANOS			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de acceso al sistema informativo del Hospital Santa Inés	Sobre la creación de perfil de usuario	Acceso no autorizado y abuso de privilegios	1) El usuario debe aceptar las condiciones de confidencialidad y del uso adecuado de la información. 2) Reciba la orden de creación de usuario aprobado por la gerencia general y recursos humanos (ref. formato RRH-ALT-001) 3) Abra el gestor Active Director 4) Vaya a la pestaña usuario y presionando el botón secundario sobre la consola de administración en el menú Nuevo - Usuario 5) Llene los datos del formulario. No puede haber dos usuarios con el mismo nombre, ni mismo nombre de cuenta. 6) Presione el botón siguiente y el asistente nos pedirá que ingresemos la contraseña. 7) Asigne la contraseña 123456789 8) Seleccione el casillero el usuario debe cambiar la contraseña al iniciar una sesión de nuevo 8) Asigne equipo de cómputo
	Sobre la modificación de perfil de usuario		1) Reciba la orden de modificación de usuario aprobado por la gerencia general y recursos humanos (ref. formato RRH-ALT-001) 2) Modifique el usuario en las plataformas requeridas 3) Confirme modificación con el usuario 4) Registre la modificación en una bitácora de control (RRH-PCC-001)

RECURSOS HUMANOS			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de acceso al sistema informativo del Hospital Santa Inés	Sobre baja temporal de perfil de usuario	Acceso no autorizado y abuso de privilegios	1) Reciba la orden de eliminación temporal de usuario aprobado por la gerencia general y recursos humanos (ref. formato RRH-PCC-001) 2) Abra el gestor Active Directory 3) Vaya a la pestaña usuarios 4) Vaya a la carpeta que contiene la cuenta de usuario 5) En el panel de detalles haga clic con el botón secundario en el usuario 6) Haga clic en deshabilitar cuenta.
	Sobre baja definitiva de perfil de usuario		1) Reciba la orden de eliminación definitiva de usuario aprobado por la gerencia general y recursos humanos (ref. formato RRH-PCC-001) 2) Abra el gestor Active Directory 3) Vaya a la pestaña usuarios 4) Vaya a la carpeta que contiene la cuenta de usuario 5) En el panel de detalles haga clic con el botón secundario en el usuario 6) Haga clic en eliminar.
Sobre control y uso correcto de la contraseña	Sobre el uso correcto de la contraseña	Suplantación de identidad en el sistema	1) Debe mantener la contraseña confidencial 2) No deben divulgar ni permitir que otros utilicen su identificación. 3) La contraseña debe tener al menos una letra mayúscula, un número, caracteres especiales y letras minúsculas 4) Tener un mínimo de siete caracteres 5) No utilizar una contraseña que anteriormente haya sido registrada 6) La contraseña no debe estar basada en nada personal como nombre, cédula, teléfono, fecha de nacimiento, etc.

RECURSOS HUMANOS			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre control y uso correcto de la contraseña	Sobre la prevención para el control de la contraseña	Olvido de la contraseña	1) Está prohibido que las contraseñas se encuentren impresas , pegadas en la pantalla o en cualquier lugar donde personas no autorizadas podrían descubrir 2) En caso de que un usuario olvide su contraseña al tercer intento incorrecto se bloqueara su acceso y deberá acercarse al administrador del sistema para que le asigne una nueva contraseña.
Sobre el control de acceso al mail interno	Sobre la creación de mail del usuario	Acceso no autorizado y abuso de privilegios	1) Para la creación ingresamos a send mail 2) Ingresamos useradd "usuario" 3) Para la contraseña ingresamos passwd "clave" 4) Mail creado
Sobre el control de acceso de equipos electrónicos que no sean propiedad del hospital	Sobre la revisión del personal del Hospital Santa Inés cuando ingresen a la jornada laboral	Fuga de Información	1) Registrarse al momento de su entrada computadoras y medios de almacenamiento en el área de recepción. 2) Los equipos se retiran a la salida
	Sobre la instalación de un antivirus que bloquee los dispositivos de los equipos		1) Algunos antivirus tienen la opción para bloquear los dispositivos USB o los CD ROM para que la información no pueda ser copiada. En este caso se debe utilizar el antivirus Kaspersky.
Sobre la elaboración de Backups	Sobre la elaboración de Backups de los equipos administrativos y servidores	Pérdida de información	1) Es obligatorio realizar copias de respaldo o backups semanalmente y el último día del mes. 2) Esto lo realizará el encargado de Sistemas quien debe conocer y manejar el software usado para la generación de respaldos 3) Preparar los Backups para su traslado

RECURSOS HUMANOS			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre la elaboración de Backups	Sobre la elaboración de Backups de los equipos personales del Hospital	Pérdida de información	1) Toda la información generada diariamente debe ser almacenada en el disco duro c\: 2) Semanalmente la información debe ser respaldada en discos externos por el jefe se sistemas de acuerdo a un horario elaborado por el mismo (PCB-PEB-001) 3) Solo el personal autorizado puede utilizar Pen Drives - Memorias USB, discos externos, CD y DVD, para el manejo y traslado de información o realización de copias de seguridad
	Sobre el traslado y custodio de los respaldos realizados		1) Los Backups deberán ser trasladados a una oficina que se encuentre fuera del hospital a un rango de 3km a la redonda para de esta manera evitar la pérdida de los mismos en caso de desastres mayores. 2) Debe llenarse una hoja de ruta para saber por dónde fueron los bakcups REF. PSB-STB-001 3) Se debe definir al personal que va a ser el encargado de este proceso 4) Es necesario un permiso de gerencia para que se realice el traslado
	Sobre la prueba de los Backups		1) Mensualmente se debe hacer un simulacro de los backups, esta puede ser al azar. 2) Llenar una bitácora (ref. PEB-PMB-001)

RECURSOS HUMANOS			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Escritorio limpio	Se debe mantener el escritorio limpio después de la jornada	Pérdida de información	1) Al terminar las labores diarias, el personal debe salir del sistema de la clínica 2) Guardar y cerrar todos los archivos que estaba utilizando 3) Cerrar correctamente las aplicaciones 4) Apagar el equipo y la pantalla 5) Se deben guardar todos los documentos utilizados en los cajones respectivos 6) Dejar el escritorio limpio sin ningún tipo de información 7) El jefe inmediato hará revisiones al azar de este punto y registrara en la bitácora el cumplimiento (ref. SEC-SME-001
Sobre el control de acceso remoto	Asistencia remota	Fuga o alteración de Información	1) La dirección de sistemas es la responsable de proporcionar el servicio de acceso remoto 2) Para el caso especial de que terceros se deban conectar remotamente deben ser autorizados por la gerencia 3) Siempre debe haber una persona responsable observando durante el acceso remoto

4.3 Políticas de Hardware

HARDWARE			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de hardware	Sobre la adquisición de equipos para el hospital Santa Inés	Perdida de Información	1) Hacer una solicitud al jefe inmediato de la necesidad para que este lo solicite al Jefe de sistemas mediante una solicitud a través del formulario (ref. SAH-HAR-001) 2) El Jefe de Sistemas y la gerencia debe analizar la solicitud y en caso de aprobar pasar al personal de compras para que se realice la compra 3) Una vez realizada la compra se debe realizar la entrega al jefe inmediato del usuario llenando el formulario (ref. SAH-HAR-002) 4) La dirección de Informática deberá tener un registro de todos los equipos del Hospital
	Sobre la instalación de equipos en el hospital Santa Inés	Perdida de Información	1) Los equipos no se deben instalar sobre alfombra deben estar levantados del piso 2) Antes de hacer las conexiones se debe comprobar polaridad 3) No ubicar los equipos cerca de ventanas o donde reciban mucho sol 4) No ubicar elementos encima de los equipos 5) No ubicar los equipos en lugares húmedos o cerca de tuberías 6)La instalación solo se realizará con autorización del jefe inmediato superior y del ingeniero de sistemas

HARDWARE			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de hardware	Sobre la reubicación de equipos en el hospital Santa Inés	Fugas de Información	1) Los activos de información no pueden salir del hospital, únicamente pueden ser reubicados. 2) Internamente los equipos pueden ser reubicados , reasignados y todo aquello que implique movimientos en su ubicación con la autorización y supervisión del jefe inmediato y el jefe de sistemas 3) Los equipos no se deben instalar sobre alfombra deben estar levantados del piso 4) Antes de hacer las conexiones se debe comprobar polaridad 5) No ubicar los equipos cerca de ventanas o donde reciban mucho sol 6) No ubicar elementos encima de los equipos 7) No ubicar los equipos en lugares húmedos o cerca de tuberías 8) La instalación solo se realizará con autorización del jefe inmediato superior y del ingeniero de sistemas
	Sobre la baja de equipos en el hospital Santa Inés		1) El jefe inmediato debe realizar una solicitud para dar de baja de un equipo al jefe de sistemas 2) El jefe de sistemas debe analizar el equipo y en caso de que sea necesario dar de baja al equipo se aprobara la solicitud 3) Se dará de baja al equipo realizando los respaldos correspondientes y con aprobación gerencia 4) Destruir información utilizando mecanismo de formateo de bajo nivel

HARDWARE			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de hardware	Sobre monitoreo de equipos en el Hospital Santa Inés	Daño no intencionado del hardware	1) Está totalmente prohibido que el usuario retire la cubierta de los equipos , este trabajo se realizará cada 6 meses por el personal de sistemas y según el horario previamente realizado que se les pasará a los usuarios (ADE-MLP-001) 2) En caso de un daño de hardware el jefe inmediato debe informar inmediatamente al personal de sistemas llenando el formulario (SAS-SOF-002) 3) Si el problema es fácil de solucionar será atendido inmediatamente. 4) En caso de requerir más tiempo el usuario debe asegurarse de respaldar en backups la información que considere relevante. 5) Se procederá a pedir un permiso para llevarse el equipo a servicio técnico dentro del mismo edificio. (RDE-MEC-001) 6) En caso de que se compruebe que el daño fue por maltrato, descuido o negligencia por parte del usuario responsable, se notificará a la Gerencia mediante un reporte de incumplimiento de las políticas de seguridad. 7) Cada usuario es responsable de su equipo informático de trabajo, y en caso de que los equipos sean compartidos se asignará un responsable del mismo (ref. SCS-SME-001) 8) En caso de robo el usuario deberá dar aviso inmediato al personal de sistemas y a la administración de Inventarios de activos.
Sobre el cuidado de los equipos	Sobre eliminación de polvo del equipo	Polvo	1) Humedecer una toalla pequeña 2) Limpiar la pantalla y el CPU con cuidado de no desconectar los cables

HARDWARE			
Política	**Procedimiento**	**Amenaza**	**Actividades**
	Sobre el uso del equipo dentro del entorno de trabajo	Pérdida de información	1) No colocar objetos encima del equipo de cómputo o tapar las salidas de ventilación del CPU. 2) No comer cerca del computador 3) No tomar líquidos cerca del computador 4) No fumar
Sobre interrupción de suministros esenciales		Termine el papel	1) Diariamente revisar la cantidad de papel 2) En caso de que se esté terminando el jefe inmediato debe realizar una solicitud con anticipación a inventarios (ref. SAH-HAR-001) 3) Llenar el registro de abastecimiento de suministros (ref. ISE-RHP-001)
		Termine el tóner	1) Tomar en cuenta el aviso del equipo de que se está terminando en tóner de la impresora 2) Inmediatamente realizar la solicitud a administración (ref. SAH-HAR-001) 3) Llenar el registro de abastecimiento de suministros (ref. ISE-RHP-001)
Sobre el cableado de cada equipo	Sobre ubicar los cables de cada equipo de manera que el usuario no se enrede	Interrupción del trabajo y pérdida de información	1) El usuario debe estar pendiente de que los cables no sean pisados por otros objetos y que no estorben su comodidad, en caso de que esto no se cumpla solicitar la reubicación de cables al personal de sistemas. 2) El cable de datos del área de trabajo debe tener un máximo de 3 m entre dispositivo y jack de la pared
Sobre reubicación de equipos en el centro de cómputo	Sobre reubicar equipos	Daño, robo o mal conexión de equipos	1) Solicitar autorización al Jefe de Sistemas con un mínimo de tres días de anticipación. (RDE-MEC-001) 2) Recibir autorización 3) Proceder a la reubicación de equipos con ayuda del jefe de Sistemas medir voltaje - exposición sol polvo

HARDWARE			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre la pérdida de un equipo	Sobre la pérdida de un equipo	Robo	1) En caso de la pérdida de un equipo se debe realizar una denuncia dentro del Hospital 2) El jefe de sistemas y de seguridad debe revisar la causa de la desaparición del equipo 3) En caso de comprobarse el robo debe realizarse una denuncia de parte de la gerencia , pedir registros de salida y constatar en cámaras de seguridad 4) Hacer los trámites con la aseguradora 5) En el menor tiempo posible el operador debe retomar su trabajo
Sobre el control de acceso a un equipo de cómputo	Sobre el control de acceso a un equipo de cómputo	Pérdida de información	1) Se debe pedir permiso al propietario de la información para acceder a la misma 2) Con este permiso el Jefe de Sistemas puede acceder al equipo de cómputo con la supervisión del propietario

4.4 Políticas de Software

SOFTWARE			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de software	Sobre la adquisición de software para el hospital Santa Inés	Pérdida de información	1) Solicitar al Jefe de sistemas mediante una solicitud la necesidad (ref. SAH-HAR-001) 2) El Jefe de Sistemas debe analizar la solicitud y en caso de aprobar pasar al personal de compras para que se realice la compra 3) Únicamente se debe comprar software con su respectiva licencia, de otra forma no se podrá instalar en los equipos 4) En caso de que el software requerido sea libre deberá obtenerse de sitios oficiales y seguros 5) Una vez realizada la compra o descargada se debe realizar la entrega al Jefe de Sistemas para que este realice la instalación en los equipos
	Sobre la instalación de software en los equipos del centro de cómputo en el hospital Santa Inés	Pérdida de información	1) En caso de que el encargado de sistemas requiera la instalación de software, deberán justificar su uso y solicitar su autorización a su jefe inmediato. (SAS-SOF-001) 2) Únicamente se permitirá la instalación de software con licencias y de acuerdo a la propiedad intelectual para los servidores y equipos del Centro de procesamiento de Datos (Centro de Cómputo). 3) En caso de necesitar reinstalar un programa se debe borrar completamente la versión instalada, para luego instalar la nueva versión. 4) Es responsabilidad del jefe de sistemas que todas las licencias se encuentren al día 5) Para proteger la integridad de los sistemas informáticos es imprescindible que todos los equipos cuenten con software de seguridad (antivirus, vacunas, privilegios de acceso , entre otros)

SOFTWARE			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de software	Sobre la instalación de software las computadoras del personal en el Hospital Santa Inés	Pérdida de información	1) En caso de que los usuarios requieran la instalación de software, deberán justificar su uso y solicitar su autorización a jefe de sistemas. (SAS-SOF-001) donde se instalara y periodo de tiempo 2) El usuario no está autorizado para instalar software en sus computadoras, esto será considerado una falta grave y se levantara un reporte de incumplimiento de las políticas de seguridad. 3) En caso de necesitar reinstalar un programa el técnico debe borrar completamente la versión instalada, para luego instalar la nueva versión. 4) Es responsabilidad del jefe de sistemas brindar asesoría y supervisión en la instalación de software informático además de que todas las licencias se encuentren al día 5) Para proteger la integridad de los sistemas informáticos es imprescindible que todos los equipos cuenten con software de seguridad (antivirus, vacunas, privilegios de acceso , entre otros)
	Sobre el traslado de equipos en el hospital Santa Inés		1) El software adquirido por el Hospital Santa Inés únicamente puede ser trasladado al local fuera del mismo donde se encuentran los backups 2) Internamente el software únicamente puede ser trasladados con la autorización y supervisión del jefe de sistemas

SOFTWARE			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de software	Sobre la baja de equipos en el hospital Santa Inés	Pérdida de información	1) El usuario debe realizar una solicitud para dar de baja al software que tenga en su computador y sea obsoleto al jefe de sistemas 2) El jefe de sistemas debe analizar el equipo y en caso de que sea necesario eliminar el software 3) El usuario no puede eliminar ningún tipo de software del equipo ya que si no se realiza correctamente este podría provocar un daño. 4) lLa desinstalación de software debe ser guardada en bitácora
	Sobre monitoreo de equipos en el Hospital Santa Inés	Daño no intencionado de la padre de software por errores en los registros	1) En caso de un daño de un programa o del sistema se debe informar inmediatamente al personal de sistemas llenando un informe (SAS-SOF-002) 2) Si el problema es fácil de solucionar será resuelto inmediatamente. 3) En caso de requerir más tiempo el usuario debe asegurarse de respaldar en backups la información que considere relevante. 4) Se procederá a pedir un permiso para llevarse el equipo a servicio técnico dentro del edificio. (RDE-MEC-001) 5) En caso de que se compruebe que el daño fue por maltrato, descuido o negligencia por parte del usuario responsable, se le levantara un reporte de incumplimiento de las políticas de información. Por lo tanto toda la información que ingrese al computador deber ser previamente analizado por el antivirus .

SOFTWARE			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre el control de software	Sobre monitoreo de equipos en el Hospital Santa Inés	Daño no intencionado de la parte de software por código malicioso	1) En caso de un daño de un programa o del sistema por código malicioso como virus, caballos de Troya o gusanos de red se debe informar inmediatamente al personal de sistemas llenando un informe (SAS-SOF-002) 2) Si el problema es fácil de solucionar será resuelto inmediatamente. 3) En caso de requerir más tiempo el usuario debe asegurarse de respaldar en backups la información que considere relevante. 4) Se procederá a pedir un permiso para llevarse el equipo a servicio técnico ya sea en el mismo edificio. (RDE-MEC-001) 5) En caso de que se compruebe que el daño fue por maltrato, descuido o negligencia por parte del usuario responsable, se le levantara un reporte de incumplimiento de las políticas de seguridad.
Sobre la actualización del software	Sobre actualización del software	Código malicioso	1) La actualización de software de todos los equipos se realizarán de acuerdo a la calendarización que anualmente sea propuesta
	Sobre actualización de antivirus		1) Revisar diariamente si el antivirus se está actualizando correctamente 2) Para esto seleccione el icono de su programa de antivirus que se encuentra en la barra de herramientas.
Sobre el control de acceso a los sistemas	Sobre acceso a los sistemas administrativos	Pérdida de información	1) Tendrá acceso solo personal que tenga autorización del responsable para apoyo técnico 2) La información administrativa que sea de uso restringido tiene que estar cifrada para garantizar su integridad

SOFTWARE			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre la administración del antivirus	Sobre la instalación del antivirus	Código malicioso	1) Antes de instalar el antivirus se debe asegurar de que no exista otro instalado en el equipo 2) Asegurarse de que el antivirus cuenta con las licencias 3) Ejecute una vacuna para identificación y eliminación de virus y similares previa la instalación de la herramienta antivirus
	Sobre el mantenimiento del antivirus		1) Realizar las actualizaciones necesarias para mantener el antivirus al día 2) En caso de que el antivirus se vuelva obsoleto buscar un nuevo antivirus 3) Desde el servidor principal del antivirus se puede instalar y desinstalar la aplicación de todos los equipos

4.5 Políticas de Redes de Comunicaciones

Redes de Comunicaciones			
Política	**Procedimiento**	**Amenaza**	**Actividades**
Sobre control de uso de las redes	Sobre el control de uso del internet	Mal uso de los recursos	1) El uso de internet queda restringido para las actividades relacionadas con el trabajo. 2) El Ingeniero de sistemas tiene la autorización de bloquear determinadas páginas y palabras y esto debe ser registrado en el respectivo documento (RDC-UDI-001) 3) Los usuarios de internet están sujetos a ser monitoreados acerca de sus actividades, está prohibido la descarga de software, música, películas y otro contenido con derechos de autor, sin autorización y el uso del mismo para fines personales. 4) Está prohibido el uso de los equipos para juegos y diversión.
	Sobre el control de uso de teléfono, correo electrónico , fax		1) El uso del teléfono, correo electrónico y fax está permitido únicamente para actividades de trabajo. 2) El uso personal de forma ocasional está permitido, siempre y cuando consuma una mínima cantidad de tiempo y recursos.

Capítulo 5

Plan de Pruebas, capacitación, control y retroalimentación

Objetivos

- Cumplir con las políticas de seguridad propuestas para evitar sanciones tanto a los administrativos como a los empleados que no cumplan con las normas.
- Garantizar que el personal cumpla con las políticas normas y procedimientos de seguridad de la información
- Garantizar que los sistemas cumplan con las políticas normas y procedimientos de seguridad de la información
- Revisar la seguridad de los sistemas de información periódicamente para garantizar el funcionamiento correcto del Hospital Santa Inés
- Garantizar la existencia de controles que protejan los activos de información del Hospital

Para cumplir con estos objetivos propuestos se presenta un plan de pruebas con tiempos de respuesta esperados, capacitaciones y controles. Cada política cuenta con un plan donde se muestran los puntos principales para ver si se cumple o no se cumple con lo esperado.

En el plan de pruebas contra incendios, terremotos, inundaciones la persona designada para realizar la prueba debe llenar el tiempo esperado, siendo el tiempo total de diez minutos para que se cumpla correctamente lo propuesto. En los demás planes de pruebas se debe tratar de que todas las actividades se cumplan para que consiga un funcionamiento óptimo. Los planes se presentan en el Anexo 3

Capítulo 6

Análisis del costo beneficio

Análisis del costo beneficio

Para el análisis del costo beneficio se debe analizar cuál sería la pérdida en caso de que una amenaza ocurriera, ya que la información del Hospital Santa Inés sufriría un impacto. Por esto el análisis del costo beneficio es una técnica que nos ayuda a tomar decisiones. Este análisis consiste en comparar el valor de la información de la empresa contra los costos de las medidas de seguridad.

En este análisis está delimitada la información mantenida en el centro de cómputo, y se calculará el impacto que produciría el robo de la misma, ya que este podría ser catastrófica si llegara a manos equivocadas, ya que contienen datos personales de los pacientes, por esta razón es importante contar con medidas de seguridad, como por ejemplo una cerradura biométrica en el centro de cómputo donde es costo esta alrededor de los $300 dólares o un sistema de detección de intrusos en caso de que una persona externa quisiera ingresar al sistema del hospital, y esto comparado con el valor de la información es insignificante así que es conveniente hacer la pequeña inversión.

Por otro lado en lo que es hardware y software es importante dar capacitaciones básicas al personal del hospital, para de esta manera evitar que la información sufra daños no intencionados. Además que el antivirus tenga las licencias actualizadas y que funcionen correctamente ya que este también podría producir costos adicionales como por ejemplo el hecho de tener que llamar a un técnico para que de mantenimiento a los computadores, este tiene un costo de 20 dólares la hora, el hecho de que para dar mantenimiento a los equipos informáticos del Hospital Santa Inés no solo se necesitaría un técnico sino más, el personal no puede laborar normalmente, el riesgo de que los equipos no queden bien configurados, el costo de tener que hacer que los usuarios de los equipos deban ir a trabajar en otros puestos, la posibilidad de que la información almacenada en los equipos se pierda, etc. Estos costos también son menores al valor de la información manejada.

Por todo esto es necesario realizar el análisis presentado a continuación:

EDIFICACIÓN				
Política	**Amenaza**	**Costo de la información (Valorado por Hospital Santa Inés)**	**Contramedidas**	**Costo de la contramedidas al año ***
Sobre el control de las instalaciones del centro de procesamiento de datos	Incendio	$ 2.000.000,00	Controles trimestrales de las instalaciones	$ 1.000,00
			Adquirir muebles no combustibles y productos de oficina metálicos	$ 500,00
			Controles trimestrales de los extintores	$ 300,00
			Instalación de detectores de humo y sistema de alarma	$ 300,00
			Instalación de sistema contra incendios a base de gas	$ 800,00
			Capacitaciones en caso de evacuaciones	$ 400,00
	Evento de cortocircuito		Control trimestrales del cableado estructurado del Centro de Cómputo	$ 1.000,00
	Evento de gotera e inundación		Control trimestrales de las instalaciones, vías y conductos de ventilación	$ 1.000,00
			Revisión trimestral de las tuberías de agua	$ 1.000,00
	Terremoto		Fijar los muebles al piso	$ 200,00

EDIFICACIÓN				
Política	**Amenaza**	**Costo de la información (Valorado por Hospital Santa Inés)**	**Contramedidas**	**Costo de la contramedidas al año ***
	Terremoto	$ 2.000.000,00	Capacitaciones en caso de evacuaciones	$ 400,00
			Controles trimestrales de las instalaciones	$ 1.000,00
			Colocar una película o film en los cristales	$ 400,00
	Evento de corte eléctrico		Instalar UPS en los servidores y computadoras del Centro de Cómputo	$ 400,00
			Revisión trimestral del generador eléctrico	$ 500,00
			Revisión trimestral de los UPS	$ 400,00
	Evento de sobrecarga eléctrica		Revisión mensual de las líneas	$ 1.000,00
Sobre el control de acceso a las instalaciones del centro de cómputo	Robo o daño de la información	$ 1.000.000,00	Instalación de cerraduras biométrica	$ 300,00
Sobre el control de acceso a las áreas restringidas del Hospital Santa Inés	Suplantación de la identidad de un usuario	$ 100.000,00	Sistema de detección de intrusos	$ 1.200,00
Sobre la señalización del hospital	Desastres naturales	$ 1.000.000,00	Instalación de las señales de emergencia	$ 500,00

* Costo de revisiones basados en hora/hombre

HARDWARE				
Política	**Amenaza**	**Costo de la información (Valorado por Hospital Santa Inés)**	**Contramedidas**	**Costo de la contramedidas al año ***
Sobre el control de hardware	Fugas de Información	$ 2.000.000,00	Capacitaciones básicas sobre informática	$ 400,00
	Daño no intencionado del hardware			
Sobre el cuidado de los equipos	Polvo		Contratar personal externo para arreglos de hardware	$ 400,00
	Pérdida de información			
Sobre interrupción de suministros esenciales	Termine el papel		Comprar con anticipación	$ 100,00
	Termine el tóner			
Sobre el cableado de cada equipo	Interrupción del trabajo y pérdida de información		Capacitaciones básicas sobre informática	$ 400,00
Sobre reubicación de equipos en el centro de cómputo	Daño, robo o mal conexión de equipos			
Sobre la pérdida de un equipo	Robo			
Sobre el control de acceso a un equipo de cómputo	Pérdida de información			

* Costo de revisiones basados en hora/hombre

SOFTWARE				
Política	**Amenaza**	**Costo de la información (Valorado por Hospital Santa Inés)**	**Contramedidas**	**Costo de la contramedidas al año ***
Sobre el control de software	Pérdida de información	$ 2.000.000,00	Creación de respaldos	$ 500,00
	Daño no intencionado de la padre de software por errores en los registros		Instalación de antivirus y las licencias anuales	$ 1.200,00
	Daño no intencionado de la parte de software por código malicioso		Instalación de un sistema de detección de intrusos	$ 1.200,00
Sobre la actualización del software	Código malicioso		Instalación de antivirus y las licencias anuales	$ 1.200,00
Sobre el control de acceso a los sistemas	Pérdida de información			
Sobre la administración del antivirus	Código malicioso		Instalación de un sistema de detección de intrusos	$ 1.200,00

* Costo de revisiones basados en hora/hombre

REDES DE COMUNICACIONES				
Política	**Amenaza**	**Costo de la información (Valorado por Hospital Santa Inés)**	**Contramedidas**	**Costo de la contramedidas al año ***
Sobre control de uso de las redes	Mal uso de los recursos	$ 2.000.000,00	Sistema de control de las redes desde el centro de cómputo	$ 500,00

* Costo de revisiones basados en hora/hombre

Como conclusión se ha llegado a que cuando el costo de la información es mayor al costo de las contramedidas lo que se debe hacer es aplicarlas ya que el valor de la información es mucho más elevado y es conveniente protegerla.

CONCLUSIONES

La Seguridad de la Información aún no es considerada por los altos directivos como uno de los aspectos más importantes en las empresas de nuestro país, pero a medida que la nueva generación de gerentes, la introducción de las TICs a las empresas, y el impulso de una sociedad virtualmente comunicada, hace que las organizaciones vean cada vez más importante y necesaria la protección de los activos de información.

Las Políticas de Seguridad de la Información son una forma de establecer las reglas de comportamiento de los usuarios, plataformas tecnológicas y proveedores de servicio, con la información de la empresa ya que establecen el cómo se debería actuar en diferentes situaciones y así mitigar los riesgos de los activos de información.

Pero para que estos procedimientos funcionen adecuadamente, dicho manual de políticas debe estar al alcance de todos y además debe ser concientizado a través de capacitaciones y talleres, para así disminuir el impacto que las amenazas podrían ocasionar.

La Seguridad de la Información del hospital Santa Inés tiene muchos puntos buenos y otros que se deben fortalecer. Por ejemplo un elemento importante que se debería tener más en cuenta es el cableado estructurado en el Centro de Cómputo ya que se encuentra desordenado, y mejorando este punto aumentaría la seguridad, la optimización y el desempeño de toda la red. El control de acceso a los diferentes departamentos, también se debería llevar de forma mejor ya que nadie sabe quién entra y sale de los departamentos.

No existía un plan de contingencia para el caso de accidentes naturales, ni un plan de emergencia ante la caída del sistema. Algo muy importante también es la capacitación del personal para el uso del hardware y software básico de la empresa ya que de esta manera se disminuiría el riesgo de daños por negligencia de los usuarios.

Mejorando estos puntos, el Hospital Santa Inés estaría asegurando de que la información se encuentra fuera de peligro.

RECOMENDACIONES

Implementar un plan de contingencia para la Seguridad de la Información, ya que esta es una herramienta imprescindible para la protección de la información, tanto lógica como física, además se debería desarrollar e implementar un plan de emergencia y un plan de recuperación de la información.

Capacitar a todo el personal del hospital, tanto administrativo como operativo, con cursos de formación periódicos, en intervalos semestrales acerca de las Políticas de Seguridad de la Información resueltas, para que de esta manera todos conozcan lo que se debe y no hacer, o cómo actuar en determinadas situaciones.

Definir los permisos y accesos de todos los usuarios del hospital, accesos físicos a los departamentos y también accesos al sistema informático. Además definir claramente las condiciones en cuanto al acceso a Internet.

Las políticas de Seguridad de la Información deben ser actualizadas periódicamente, esto debería estar a cargo de un comité de Seguridad de la Información, en el que debería participar el propietario de información de cada área del hospital.

Se deben realizar simulacros cada tres meses, para saber cómo actuar ante desastres naturales como incendios, inundaciones o terremotos, de esta manera el personal del hospital sabrá cómo actuar en estas situaciones.

La seguridad física de la puerta del Centro de Cómputo debería ser tomada en cuenta y contener una cerradura electrónica, además se recomienda implementar un sistema de refrigeración en el Centro de Cómputo para mantener a los equipos dentro de los márgenes térmicos recomendados por el fabricante de hardware.

ANEXOS

Anexo 1

Entrevistas

PERSONAL

Código Empleado:		Fecha:	
Nombre:			
Departamento:		Cargo:	
Proceso:			

HARDWARE

Nombre Equipo:		IP:	
Serie Equipo:			
Confidencialidad:			
Disponibilidad:			
Integridad:			

SOFTWARE

# Licencia Windows:	
# Licencia Office:	
# Licencia Antivirus:	
# Licencia Otros:	

SISTEMA CLINICA

Información Electrónica disponible		
	Historial de la Clínica	
	Contabilidad	
	Financiero	
	Enfermería	
	Activos fijos	
	Economato (Bodegas y compras)	
	Caja Medica	
	Facturación	
	Hospitalización	

	Emergencia	
	Bancos	
	Botica	
	Quirófanos	
	Otros	

DOCUMENTOS
PAPEL

Descripción	
Confidencialidad:	
Disponibilidad:	
Integridad:	

EDIFICACION

Departamento:			Alta, Baja
Planta:			
Confidencialidad:			
Disponibilidad:			
Integridad:			

MEDIOS DE RESPALDO

SERVICIOS

Tipo servicio:		Fecha Firma:	
Tipo Contrato:		Fecha Expiración:	
Proveedor:			

Anexo 2

Matriz de Software

ID SOFT	Código Empleado	Empleado	Nombre Equipo	Tipo de Software	Software	Licencia	Procesos
[SW][OS]1	[P][OP]1	BELÉN PAREDES	HOSTELERÍA	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	3.1-3.2
[SW][OFFICE]1	[P][OP]1	BELÉN PAREDES	HOSTELERÍA	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	3.1-3.2
[SW][OS]2	[P][OP]2	MA. EUGENIA PLAZA	CAJA	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	13.2
[SW][OFFICE]2	[P][OP]2	MA. EUGENIA PLAZA	CAJA	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	13.2
[SW][OS]3	[P][OP]3	MA. ISABEL SOLORZANO	SEGUROS	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	12.2
[SW][OFFICE]3	[P][OP]3	MA. ISABEL SOLORZANO	SEGUROS	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	12.2
[SW][OS]4	[P][OP]4	LORENA ENDERICA	FARMACIA_DRA	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	5

ID SOFT	Código Empleado	Empleado	Nombre Equipo	Tipo de Software	Software	Licencia	Procesos
[SW][OFFICE]4	[P][OP]4	LORENA ENDERICA	FARMACIA_DRA	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	5
[SW][OS]5	[P][OP]5	TANIA SAVALA	BOTICA-DSCRG	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	5.1-5.2-13.2
[SW][OFFICE]5	[P][OP]5	TANIA SAVALA	BOTICA-DSCRG	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	5.1-5.2-13.2
[SW][OS]6	[P][OP]6	ALEJANDRA ESPINA	BOTICA_FACTURA	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	5.1-5.2-13.2
[SW][OFFICE]6	[P][OP]6	ALEJANDRA ESPINA	BOTICA_FACTURA	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	5.1-5.2-13.2
[SW][OS]7	[P][OP]7	LILENA MUÑOZ	FERCAL	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	12
[SW][OFFICE]7	[P][OP]7	LILENA MUÑOZ	FERCAL	OFFICE	Office Professional Pluss 2007	VB48G-H6VK9-WJ93D-9R6RM-VP7GT	12
[SW][OS]8	[P][OP]8	PAOLA CHICA	CONVENIOS	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	12

ID SOFT	Código Empleado	Empleado	Nombre Equipo	Tipo de Software	Software	Licencia	Procesos
[SW][OFFICE]8	[P][OP]8	PAOLA CHICA	CONVENIOS	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	12
[SW][OS]9	[P][OP]9	DIANA SUAREZ	CAJATESORERIA	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	12
[SW][OFFICE]9	[P][OP]9	DIANA SUAREZ	CAJATESORERIA	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	12
[SW][OFFICE]10	[P][OP]9	DIANA SUAREZ	CAJATESORERIA	OFFICE	Office Enterprise 2007	VB48G-H6VK9-WJ93D-9R6RM-VP7GT	12
[SW][OS]10	[P][OP]10	JOHANA MOSQUERA	COMPRAS	OS	WINDOWS XP	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	14
[SW][OFFICE]11	[P][OP]10	JOHANA MOSQUERA	COMPRAS	OFFICE	Office Enterprise 2007	VB48G-H6VK9-WJ93D-9R6RM-VP7GT	14
[SW][OS]11	[P][OP]11	FERNANDA NIVICELA	MXSANTAINES	OS	LINUX CENTOS 6.0	GNU	1.2-2.1-3.1-4.1-4-3-4.4-5.1-5.2-6.1-6.2-18-7.2-11.1-11.3-11.4-12.1-12.2-13-14-15.1-16.1-17.1-17.2-17.3-19-20.1-20.2-21.1-21.2-21.3

ID SOFT	Código Empleado	Empleado	Nombre Equipo	Tipo de Software	Software	Licencia	Procesos
[SW][OFFICE]12	[P][OP]11	FERNANDA NIVICELA	MXSANTAINES	OFFICE	Open Office	Gratis	1.2-2.1-3.1-4.1-4-3-4.4-5.1-5.2-6.1-6.2-18-7.2-11.1-11.3-11.4-12.1-12.2-13-14-15.1-16.1-17.1-17.2-17.3-19-20.1-20.2-21.1-21.2-21.3
[SW][AV]1	[P][OP]11	FERNANDA NIVICELA	MXSANTAINES	AV	Kaspersky		1.2-2.1-3.1-4.1-4-3-4.4-5.1-5.2-6.1-6.2-18-7.2-11.1-11.3-11.4-12.1-12.2-13-14-15.1-16.1-17.1-17.2-17.3-19-20.1-20.2-21.1-21.2-21.3
[SW][EMAIL_CLIENT]1	[P][OP]11	FERNANDA NIVICELA	MXSANTAINES	EMAIL_CLIENT	Send MaiL		1.2-2.1-3.1-4.1-4-3-4.4-5.1-5.2-6.1-6.2-18-7.2-11.1-11.3-11.4-12.1-12.2-13-14-15.1-16.1-17.1-17.2-17.3-19-20.1-20.2-21.1-21.2-21.3
IDSOFT26	[P][OP]11	FERNANDA NIVICELA	MXSANTAINES		Dovecot		1.2-2.1-3.1-4.1-4-3-4.4-5.1-5.2-6.1-6.2-18-7.2-11.1-11.3-11.4-12.1-12.2-13-14-15.1-16.1-17.1-17.2-17.3-19-20.1-20.2-21.1-21.2-21.3
[SW][OS]12	[P][OP]11	FERNANDA NIVICELA	PROXY 01	OS	ZENTYAL	EDICION COMUNIDAD	21.3
[SW][OS]13	[P][OP]11	FERNANDA NIVICELA	PROXY PUB	OS	ZENTYAL	EDICION COMUNIDAD	21.3

ID SOFT	Código Empleado	Empleado	Nombre Equipo	Tipo de Software	Software	Licencia	Procesos
[SW][OS]14	[P][OP]11	FERNANDA NIVICELA	SRV	OS	WINDOWS 2003	P4B36-V34C3-G22MD-497FJ-X4WHW	21.3
[SW][OS]15	[P][OP]11	FERNANDA NIVICELA	CAMARAS 1	OS	LINUX	GNU	21.3-22.2
[SW][APP]1	[P][OP]11	FERNANDA NIVICELA	CAMARAS 1	APP	GV1000		21.3-22.2
[SW][OS]16	[P][OP]11	FERNANDA NIVICELA	CAMARAS 2	OS	LINUX	YQ7XW-QPT6C-233QF-RRXC7-VF7TY	21.3-22.2
[SW][OFFICE]13	[P][OP]11	FERNANDA NIVICELA	CAMARAS 2	OFFICE	Office XP Professional con FrontPage	FM9FY-TMF7Q-KCKCT-V9T29-TBBBG	21.3-22.2
[SW][APP]2	[P][OP]11	FERNANDA NIVICELA	CAMARAS 2	APP	GV1000		21.3-22.2
[SW][OFFICE]14	[P][OP]11	FERNANDA NIVICELA	CAMARAS 3	OS	LINUX	GNU	21.3-22.2
[SW][APP]3	[P][OP]11	FERNANDA NIVICELA	FIREWALL	APP	CHECKPOINT	3025997WBDH16RY2MKRSWNCH	21.3
[SW][AV]2	[P][OP]11	FERNANDA NIVICELA	ANTIVIRUS	ANT	KASPERSKI	LIC	21.3
[SW][OS]17	[P][OP]12	FERNANDA PIEDRA	PAGADURIA	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	4.1-4.2-4.3
[SW][OFFICE]15	[P][OP]12	FERNANDA PIEDRA	PAGADURIA	OFFICE	Office Profession	GWH28-DGCMP-P6RC4-6J4MT-	4.1-4.2-4.3

ID SOFT	Código Empleado	Empleado	Nombre Equipo	Tipo de Software	Software	Licencia	Procesos
					al Edition 2003	3HFDY	
[SW][OS]18	[P][OP]13	LORENA PEÑA	CONTABILIDAD1	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	13
[SW][OFFICE]16	[P][OP]13	LORENA PEÑA	CONTABILIDAD1	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	13
[SW][OS]19	[P][OP]14	FANNY MONTERO	CONTABILIDAD2	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	13
[SW][OFFICE]17	[P][OP]14	FANNY MONTERO	CONTABILIDAD2	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	13
[SW][OS]20	[P][OP]15	LORENA PEÑA	CONTABILIDAD3	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	13
[SW][OFFICE]18	[P][OP]15	LORENA PEÑA	CONTABILIDAD3	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	13
[SW][OS]21	[P][OP]16	JUAN ALARCÓN	JEFE-CONTA	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	13

ID SOFT	Código Empleado	Empleado	Nombre Equipo	Tipo de Software	Software	Licencia	Procesos
[SW][OFFICE]19	[P][OP]16	JUAN ALARCÓN	JEFE-CONTA	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	13
[SW][OS]22	[P][OP]17	ESTELA LEÓN	LABORATORIO2	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	6
[SW][OFFICE]20	[P][OP]17	ESTELA LEÓN	LABORATORIO2	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	6
[SW][OS]23	[P][OP]18	VERÓNICA MARIDUEÑA	EMERGENCIA1	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	11
[SW][OFFICE]21	[P][OP]18	VERÓNICA MARIDUEÑA	EMERGENCIA1	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	11
[SW][OS]24	[P][OP]19	LUIS MARIO TAMAYO	UCI01	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	1-3-7
[SW][OFFICE]22	[P][OP]19	LUIS MARIO TAMAYO	UCI01	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	1-3-7
[SW][OS]25	[P][OP]20	ELIZABETH AGUIRRE	ENFERMERIA1DOS	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	18.3

ID SOFT	Código Empleado	Empleado	Nombre Equipo	Tipo de Software	Software	Licencia	Procesos
[SW][OFFICE]23	[P][OP]20	ELIZABETH AGUIRRE	ENFERMERIA1DOS	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	18.3
[SW][OS]26	[P][OP]21	ELIZABETH AGUIRRE	RECUPERACION	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	1.6
[SW][OFFICE]24	[P][OP]21	ELIZABETH AGUIRRE	RECUPERACION	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	1.6
[SW][OS]27	[P][OP]22	ELIZABETH AGUIRRE	ENFERMERIAUNO	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	18.3
[SW][OFFICE]25	[P][OP]22	ELIZABETH AGUIRRE	ENFERMERIAUNO	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	18.3
[SW][OS]28	[P][OP]23	MÓNICA CAMPOVERDE	QUIRÓFANOS	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	1
[SW][OFFICE]26	[P][OP]23	MÓNICA CAMPOVERDE	QUIRÓFANOS	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	1
[SW][OS]29	[P][OP]24	ELIZABETH AGUIRRE	ENFERMERIA4	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	18.3

ID SOFT	Código Empleado	Empleado	Nombre Equipo	Tipo de Software	Software	Licencia	Procesos
[SW][OFFICE]27	[P][OP]24	ELIZABETH AGUIRRE	ENFERMERIA4	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	18.3
[SW][OS]30	[P][OP]25	MA. EUGENIA PLAZA	CAJA2	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	4.2-4.5
[SW][OFFICE]28	[P][OP]25	MA. EUGENIA PLAZA	CAJA2	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	4.2-4.5
[SW][OS]31	[P][OP]26	FERNABDA PIEDRA	TESORERIAP	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	4.1
[SW][OFFICE]29	[P][OP]26	FERNABDA PIEDRA	TESORERIAP	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	4.1
[SW][OS]32	[P][OP]27	ANA CRISTINA ANDRADE	ADMISIONES	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	11.5
[SW][OFFICE]30	[P][OP]27	ANA CRISTINA ANDRADE	ADMISIONES	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	11.5
[SW][OS]33	[P][OP]28	ANGÉLICA ORELLANA	ECONOMA1	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	4

ID SOFT	Código Empleado	Empleado	Nombre Equipo	Tipo de Software	Software	Licencia	Procesos
[SW][OFFICE]31	[P][OP]28	ANGÉLICA ORELLANA	ECONOMA1	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	4
[SW][OS]34	[P][OP]29	ANGÉLICA ORELLANA	COCINA_BAR	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	20
[SW][OFFICE]32	[P][OP]29	ANGÉLICA ORELLANA	COCINA_BAR	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	20
[SW][OS]35	[P][OP]30	DR ANDRES MALO	DIRMEDICA	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	18
[SW][OFFICE]33	[P][OP]30	DR ANDRES MALO	DIRMEDICA	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	18
[SW][OS]36	[P][OP]31	MÓNICA CAMPOVERDE	NEONATOLOGIA	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	7
[SW][OFFICE]34	[P][OP]31	MÓNICA CAMPOVERDE	NEONATOLOGIA	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	7
[SW][OS]37	[P][OP]32	DR VASQUEZ	CARDIO	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	2-8-9

ID SOFT	Código Empleado	Empleado	Nombre Equipo	Tipo de Software	Software	Licencia	Procesos
[SW][OFFICE]35	[P][OP]32	DR VASQUEZ	CARDIO	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	2-8-9
[SW][OS]38	[P][OP]33	ELIZABETH AGUIRRE	ENFERMERIA 3	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	18.3
[SW][OFFICE]36	[P][OP]33	ELIZABETH AGUIRRE	ENFERMERIA 3	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	18.3
[SW][OS]39	[P][OP]34	ING BRUNO LEDESMA	GERENCIA	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	18
[SW][OFFICE]37	[P][OP]34	ING BRUNO LEDESMA	GERENCIA	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	18
[SW][OS]40	[P][OP]35	BELÉN PAREDES	ATENCIONCLIENTE	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	2.2
[SW][OFFICE]38	[P][OP]35	BELÉN PAREDES	ATENCIONCLIENTE	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	2.2
[SW][OS]41	[P][OP]36	DR CRIOLLO	CRAYOSX	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	2.1-2.2

ID SOFT	Código Empleado	Empleado	Nombre Equipo	Tipo de Software	Software	Licencia	Procesos
[SW][OFFICE]39	[P][OP]36	DR CRIOLLO	CRAYOSX	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	2.1-2.2
[SW][OS]42	[P][OP]37	DRA LORENA ENDERICA	SUMCENTRAL	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	14
[SW][OFFICE]40	[P][OP]37	DRA LORENA ENDERICA	SUMCENTRAL	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	14
[SW][OS]43	[P][OP]38	ELIZABETH AGUIRRE	ENFERMERIA4DOS	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	18.3
[SW][OFFICE]41	[P][OP]38	ELIZABETH AGUIRRE	ENFERMERIA4DOS	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	18.3
[SW][OS]44	[P][OP]39	DR CRIOLLO	ECOGRAFIA01	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	3
[SW][OFFICE]42	[P][OP]39	DR CRIOLLO	ECOGRAFIA01	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	3
[SW][OS]45	[P][OP]40	DR CRIOLLO	CAJAIMAGENES	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	7

ID SOFT	Código Empleado	Empleado	Nombre Equipo	Tipo de Software	Software	Licencia	Procesos
[SW][OFFICE]43	[P][OP]40	DR CRIOLLO	CAJAIMAGENES	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	7
[SW][OS]46	[P][OP]41	DR LUIS MARIO TAMAYO	PCAISLAMIENTO	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	3
[SW][OFFICE]44	[P][OP]41	DR LUIS MARIO TAMAYO	PCAISLAMIENTO	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	3
[SW][OS]47	[P][OP]42	ELIZABETH AGUIRRE	HOSPITALIZACIÓN	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	3
[SW][OFFICE]45	[P][OP]42	ELIZABETH AGUIRRE	HOSPITALIZACIÓN	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	3
[SW][OS]48	[P][OP]43	LUIS MARIO TAMAYO	UCI	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	18.3
[SW][OFFICE]46	[P][OP]43	LUIS MARIO TAMAYO	UCI	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	18.3
[SW][OS]49	[P][OP]44	DRA M EUGENIA SUARES	SECREGERENCIA	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	19

ID SOFT	Código Empleado	Empleado	Nombre Equipo	Tipo de Software	Software	Licencia	Procesos
[SW][OFFICE]47	[P][OP]44	DRA M EUGENIA SUARES	SECREGERENCIA	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	19
[SW][OS]50	[P][OP]45	FERNANDA NIVICELA	ZENTYAL PROXY 01	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	1.2-2.1-3.1-4.1-4-3-4.4-5.1-5.2-6.1-6.2-18-7.2-11.1-11.3-11.4-12.1-12.2-13-14-15.1-16.1-17.1-17.2-17.3-19-20.1-20.2-21.1-21.2-21.3
[SW][OFFICE]48	[P][OP]45	FERNANDA NIVICELA	ZENTYAL PROXY 01	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	1.2-2.1-3.1-4.1-4-3-4.4-5.1-5.2-6.1-6.2-18-7.2-11.1-11.3-11.4-12.1-12.2-13-14-15.1-16.1-17.1-17.2-17.3-19-20.1-20.2-21.1-21.2-21.3
[SW][OS]51	[P][OP]46	FERNANDA CRIOLLO	CARTERA_SEGUROS	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	12.2
[SW][OFFICE]49	[P][OP]46	FERNANDA CRIOLLO	CARTERA_SEGUROS	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	12.2
[SW][OS]52	[P][OP]47	ELIZABETH AGUIRRE	NVASVR	OS	WINDOWS XP	KYKVX-86GQG-2MDY9-F6J9M-K42BQ	

ID SOFT	Código Empleado	Empleado	Nombre Equipo	Tipo de Software	Software	Licencia	Procesos
[SW][OFFICE]50	[P][OP]47	ELIZABETH AGUIRRE	NVASVR	OFFICE	Office Professional Edition 2003	GWH28-DGCMP-P6RC4-6J4MT-3HFDY	

Matriz de Hardware

ID HARD	Código Empleado	Empleado	Tipo activo	Nombre Equipo	Dirección Mac	IP	Confidencialidad	Disponibilidad	Integridad
[HW][PC]1	[P][OP]1	BELÉN PAREDES	PC	HOSTELERÍA	00-16-35-68-09-E6	192.168.1.148	2	1	3
[HW][PC]2	[P][OP]2	MA. EUGENIA PLAZA	PC	CAJA	00-16-35-AB-8A-3B	192.168.1.138	2	3	3
[HW][PC]3	[P][OP]3	MA. ISABEL SOLORZANO	PC	SEGUROS	00-14-C2-C8-58-E3	192.168.1.39	2	2	3
[HW][PC]4	[P][OP]4	LORENA ENDERICA	PC	FARMACIA_DRA	00-14-C2-C9-74-B4	192.168.1.165	1	2	3
[HW][PC]5	[P][OP]5	TANIA SAVALA	PC	BOTICA-DSCRG	00-16-35-68-17-AD	192.168.1.220	2	3	3
[HW][PC]6	[P][OP]6	ALEJANDRA ESPINA	PC	BOTICA_FACTURA	00-16-35-68-0B-0D	192.168.1.83	2	3	3
[HW][PC]7	[P][OP]7	LILENA MUÑOZ	PC	FERCAL	00-14-C2-C8-88-80	192.168.1.156	3	3	3
[HW][PC]8	[P][OP]8	PAOLA CHICA	PC	CONVENIOS	E0-69-95-9A-1D-ED	192.168.1.121	2	3	3
[HW][PC]9	[P][OP]9	DIANA SUAREZ	PC	CAJATESORERIA	00-16-35-68-13-A9	192.168.1.146	3	3	3
[HW][PC]10	[P][OP]10	JOHANA	PC	COMPRAS	90-FB-A6-	192.168.	2	2	3

ID HARD	Código Empleado	Empleado	Tipo activo	Nombre Equipo	Dirección Mac	IP	Confidencialidad	Disponibilidad	Integridad
		MOSQUERA			33-04-EC	1.24			
[HW][PC]11	[P][OP]11	FERNANDA NIVICELA	PC	MXSANTAINES	70-71-BC-8F-F0-F8	192.168.1.6	3	3	3
[HW][PC]12	[P][OP]11	FERNANDA NIVICELA	PC	PROXY 01	E0-69-95-3B-A9-12	192.168.1.212	3	3	3
[HW][PC]13	[P][OP]11	FERNANDA NIVICELA	PC	PROXY PUB	00-1C-C0-BC-71-07	192.168.10.2	3	3	3
[HW][ELECTRONIC][DISK]1	[P][OP]11	FERNANDA NIVICELA	DISK	SRV	00-16-35-AC-A5-95	192.168.1.254	3	3	3
[HW][ELECTRONIC][DISK]2	[P][OP]11	FERNANDA NIVICELA	DISK	CAMARAS 1	00-40.48-81-29-06	192.168.10.11	3	3	3
[HW][ELECTRONIC][DISK]3		FERNANDA NIVICELA	DISK	CAMARAS 2	00-40-48-87-12-F0	192.168.10.12	3	3	3
[HW][ELECTRONIC][DISK]4	[P][OP]11	FERNANDA NIVICELA	DISK	CAMARAS 3	00-40-48-87-13-01	192.168.10.13	3	3	3
[HW][NETWORK][FIREWALL]1	[P][OP]11	FERNANDA NIVICELA	PC	FIREWALL	00-08-DA-54-8A-F1	192.168.1.253	3	3	3
[HW][PC]14	[P][OP]11	FERNANDA NIVICELA	PC	ANTIVIRUS	70-71-BC-8F-F0-F0	192.168.1.252	3	3	3
[HW][PC]15	[P][OP]12	FERNANDA PIEDRA	PC	PAGADURIA	00-16-35-AC-A5-8A	192.168.1.155	2	3	3
[HW][PC]16	[P][OP]13	LORENA PEÑA	PC	CONTABILIDAD1	00-14-C2-C9-77-C9	192.168.1.179	3	3	3
[HW][PC]17	[P][OP]14	FANNY MONTERO	PC	CONTABILIDAD2	00-16-35-68-17-97	192.168.1.77	3	3	3
[HW][PC]18	[P][OP]15	LORENA PEÑA	PC	CONTABILIDAD3	00-16-35-AB-89-F4	192.168.1.172	3	3	3
[HW][PC]19	[P][OP]16	JUAN ALARCÓN	PC	JEFE-CONTA	00-14-C2-C8-8A-3C	192.168.1.42	3	3	3

ID HARD	Código Empleado	Empleado	Tipo activo	Nombre Equipo	Dirección Mac	IP	Confidencialidad	Disponibilidad	Integridad
[HW][PC]20	[P][OP]17	ESTELA LEÓN	PC	LABORATORIO2	00-14-C2-C8-89-AB	192.168.1.160	3	3	3
[HW][PC]21	[P][OP]17	VERÓNICA MARIDUEÑA	PC	EMERGENCIA1	00-16-35-68-16-0C	192.168.1.128	2	3	3
[HW][PC]22	[P][OP]18	LUIS MARIO TAMAYO	PC	UCI01	90-FB-A6-8B-85-36	192.168.1.119	3	3	3
[HW][PC]23	[P][OP]18	LUIS MARIO TAMAYO	PC	ENFERMERIA1DOS	00-16-35-AB-85-C3	192.168.1.130	2	2	3
[HW][PC]24	[P][OP]19	ELIZABETH AGUIRRE	PC	RECUPERACION	00-16-35-68-17-A3	192.168.1.134	2	3	3
[HW][PC]25	[P][OP]19	ELIZABETH AGUIRRE	PC	ENFERMERIAUNO	00-16-35-68-17-19	192.168.1.133	2	3	3
[HW][PC]26	[P][OP]20	ELIZABETH AGUIRRE	PC	QUIRÓFANOS	00-17-A4-42-2A-6A	192.168.1.135	3	3	3
[HW][PC]27	[P][OP]20	ELIZABETH AGUIRRE	PC	ENFERMERIA4	00-16-35-AC-A5-74	192.168.1.137	2	3	3
[HW][PC]28	[P][OP]21	ELIZABETH AGUIRRE	PC	CAJA2	00-17-A4-42-29-2D	192.168.1.139	2	3	3
[HW][PC]29	[P][OP]21	ELIZABETH AGUIRRE	PC	TESORERIAP	00-14-C2-C8-22-B8	192.168.1.149	3	3	3
[HW][PC]30	[P][OP]22	MÓNICA CAMPOVERDE	PC	ADMISIONES	00-14-C2-C8-59-57	192.168.1.147	2	2	3
[HW][PC]31	[P][OP]22	MÓNICA CAMPOVERDE	PC	ECONOMA1	00-16-35-68-17-0C	192.168.1.150	2	3	3
[HW][PC]32	[P][OP]23	ELIZABETH AGUIRRE	PC	COCINA_BAR	00-16-35-AB-88-53	192.168.1.151	1	1	1
[HW][PC]33	[P][OP]23	ELIZABETH AGUIRRE	PC	DIRMEDICA	78-E3-B5-50-C4-8F	192.168.1.152	3	3	3
[HW][PC]34	[P][OP]24	MA. EUGENIA PLAZA	PC	NEONATOLOGIA	00-16-35-AB-88-AA	192.168.1.159	3	3	3

ID HARD	Código Empleado	Empleado	Tipo activo	Nombre Equipo	Dirección Mac	IP	Confidencialidad	Disponibilidad	Integridad
[HW][PC]35	[P][OP]24	MA. EUGENIA PLAZA	PC	CARDIO	90-FB-A6-33-04-B1	192.168.1.158	3	3	3
[HW][PC]36	[P][OP]25	FERNABDA PIEDRA	PC	ENFERMERIA 3	00-14-C2-C9-74-A8	192.168.1.163	2	3	3
[HW][PC]37	[P][OP]25	FERNABDA PIEDRA	PC	GERENCIA	C8-2A-14-12-5E-D7	192.168.1.167	3	3	3
[HW][PC]38	[P][OP]26	ANA CRISTINA ANDRADE	PC	ATENCIONCLIENTE	00-16-35-68-06-2B	192.168.1.157	2	3	3
[HW][PC]39	[P][OP]26	ANA CRISTINA ANDRADE	PC	CRAYOSX	00-16-35-68-12-74	192.168.1.166	3	3	3
[HW][PC]40	[P][OP]27	ANGÉLICA ORELLANA	PC	SUMCENTRAL	E0-69-95-0D-CE-55	192.168.1.164	2	3	3
[HW][PC]41	[P][OP]27	ANGÉLICA ORELLANA	PC	ENFERMERIA4DOS	00-16-35-68-0B-F3	192.168.1.169	2	2	3
[HW][PC]42	[P][OP]28	ANGÉLICA ORELLANA	PC	ECOGRAFIA01	38-60-77-CE-32-F0	192.168.1.175	3	3	3
[HW][PC]43	[P][OP]28	ANGÉLICA ORELLANA	PC	CAJAIMAGENES	00-14-2A-02-36-F0	192.168.1.180	2	3	3
[HW][PC]44	[P][OP]29	DR ANDRES MALO	PC	PCAISLAMIENTO	00-03-47-CC-CF-B0	192.168.1.188	3	3	3
[HW][PC]45	[P][OP]29	DR ANDRES MALO	PC	HOSPITALIZACIÓN	00-16-35-AB-88-89	192.168.1.141	2	3	3
[HW][PC]46	[P][OP]30	MÓNICA CAMPOVERDE	PC	UCI	00-16-35-68-14-FA	192.168.1.199	3	3	3
[HW][PC]47	[P][OP]30	MÓNICA CAMPOVERDE	PC	SECREGERENCIA	00-14-C2-C9-73-63	192.168.1.201	2	2	3
[HW][PC]48	[P][OP]31	DR VASQUEZ	PC	ZENTYAL PROXY 01	E0-69-95-3B-A9-12	192.168.1.212	3	3	3
[HW][PC]49	[P][OP]31	DR VASQUEZ	PC	CARTERA_SEGUROS	00-16-35-68-0B-7E	192.168.1.228	2	2	3

ID HARD	Código Empleado	Empleado	Tipo activo	Nombre Equipo	Dirección Mac	IP	Confidencialidad	Disponibilidad	Integridad
[HW][PC]50	[P][OP]32	ELIZABETH AGUIRRE	PC	NVASVR	00-11-25-C5-5D-62	192.168.1.249	3	3	3
[HW][PERIPHERAL][PRINT]1	[P][OP]32	ELIZABETH AGUIRRE	PRINT	0	08-00-37-AA-EE-9A	192.168.1.25	1	1	1
[HW][PERIPHERAL][PRINT]2	[P][OP]33	ING BRUNO LEDESMA	PRINT	0	00-00-AA-99-C0-24	192.168.1.28	1	1	1
[HW][PERIPHERAL][PRINT]3	[P][OP]33	ING BRUNO LEDESMA	PRINT	0	00-00-AA-D6-E5-27	192.168.1.30	1	1	1

Matriz de edificación

ID EDIFICACION	Código Empleado	Empleado	Nombre Equipo	Departamento	Planta	Confidencialidad	Disponibilidad	Integridad
[L][BUILDING][PISO0]1	[P][OP]1	BELÉN PAREDES	HOSTELERÍA	HOTELERIA	0	3	1	2
[L][BUILDING][PISO0]2	[P][OP]2	MA. EUGENIA PLAZA	CAJA	CAJA	0	1	3	3
[L][BUILDING][PISO0]3	[P][OP]3	MA. ISABEL SOLORZANO	SEGUROS	SEGUROS	0	2	3	3
[L][BUILDING][PISO0]4	[P][OP]4	LORENA ENDERICA	FARMACIA_DRA	FARMACIA	3	3	3	3
[L][BUILDING][PISO0]5	[P][OP]5	TANIA SAVALA	BOTICA-DSCRG	FARMACIA	3	3	3	3
[L][BUILDING][PISO0]6	[P][OP]6	ALEJANDRA ESPINA	BOTICA_FACTURA	FARMACIA	3	3	3	3
[L][BUILDING][PISO5]1	[P][OP]7	LILENA MUÑOZ	FERCAL	CONVENIOS	5	3	3	3

ID EDIFICACION	Código Empleado	Empleado	Nombre Equipo	Departamento	Planta	Confidencialidad	Disponibilidad	Integridad
[L][BUILDING][PISO5]2	[P][OP]8	PAOLA CHICA	CONVENIOS	CONVENIOS	5	3	3	3
[L][BUILDING][PISO5]3	[P][OP]9	DIANA SUAREZ	CAJATESORERIA	CONVENIOS	5	3	3	3
[L][BUILDING][PISO5]4	[P][OP]10	JOHANA MOSQUERA	COMPRAS	COMPRAS	5	2	2	3
[L][BUILDING][PISO5]5	[P][OP]11	FERNANDA NIVICELA	MXSANTAINES	SISTEMAS	5	3	3	3
[L][BUILDING][PISO5]6	[P][OP]11	FERNANDA NIVICELA	PROXY 01	SISTEMAS	5	3	3	3
[L][BUILDING][PISO5]7	[P][OP]11	FERNANDA NIVICELA	PROXY PUB	SISTEMAS	5	3	3	3
[L][BUILDING][PISO5]8	[P][OP]11	FERNANDA NIVICELA	SRV	SISTEMAS	5	3	3	3
[L][BUILDING][PISO5]9	[P][OP]11	FERNANDA NIVICELA	CAMARAS 1	SISTEMAS	5	3	3	3
[L][BUILDING][PISO5]10	[P][OP]11	FERNANDA NIVICELA	CAMARAS 2	SISTEMAS	5	3	3	3
[L][BUILDING][PISO5]11	[P][OP]11	FERNANDA NIVICELA	CAMARAS 3	SISTEMAS	5	3	3	3
[L][BUILDING][PISO5]12	[P][OP]11	FERNANDA NIVICELA	FIREWALL	SISTEMAS	5	3	3	3
[L][BUILDING][PISO5]13	[P][OP]11	FERNANDA NIVICELA	ANTIVIRUS	SISTEMAS	5	3	3	3
[L][BUILDING][PISO0]7	[P][OP]12	FERNANDA PIEDRA	PAGADURIA	PAGADURIA	0	2	3	3
[L][BUILDING][PISO5]14	[P][OP]13	LORENA PEÑA	CONTABILIDAD1	CONTABILIDAD	5	3	3	3
[L][BUILDING][PISO5]15	[P][OP]14	FANNY MONTERO	CONTABILIDAD2	CONTABILIDAD	5	3	3	3

ID EDIFICACION	Código Empleado	Empleado	Nombre Equipo	Departamento	Planta	Confidencialidad	Disponibilidad	Integridad
[L][BUILDING][PISO5]16	[P][OP]15	LORENA PEÑA	CONTABILIDAD3	CONTABILIDAD	5	3	3	3
[L][BUILDING][PISO5]17	[P][OP]16	JUAN ALARCÓN	JEFE-CONTA	CONTABILIDAD	5	3	3	3
[L][BUILDING][PISO0]8	[P][OP]17	ESTELA LEÓN	LABORATORIO2	LABORATORIO	0	3	3	3
[L][BUILDING][PISO0]9	[P][OP]17	VERÓNICA MARIDUEÑA	EMERGENCIA1	EMERGENCIA	0	3	3	3
[L][BUILDING][PISO1]1	[P][OP]18	LUIS MARIO TAMAYO	UCI01	CUIDADOS INTENSIVOS	1	3	3	3
[L][BUILDING][PISO2]1	[P][OP]18	LUIS MARIO TAMAYO	ENFERMERIA1DOS	ENFERMERIA	todos	3	3	3
[L][BUILDING][PISO1]2	[P][OP]19	ELIZABETH AGUIRRE	RECUPERACION	RECUPERACION	1	3	3	3
[L][BUILDING][PISO2]2	[P][OP]19	ELIZABETH AGUIRRE	ENFERMERIAUNO	ENFERMERIA		3	3	3
[L][BUILDING][PISO1]3	[P][OP]20	ELIZABETH AGUIRRE	QUIRÓFANOS	QUIRÓFANOS	1	3	3	3
[L][BUILDING][PISO4]1	[P][OP]20	ELIZABETH AGUIRRE	ENFERMERIA4	ENFERMERIA	4	3	3	3
[L][BUILDING][PISO0]10	[P][OP]21	ELIZABETH AGUIRRE	CAJA2	CAJA	0	3	3	3
[L][BUILDING][PISO0]11	[P][OP]21	ELIZABETH AGUIRRE	TESORERIAP	TESORIA	0	3	3	3
[L][BUILDING][PISO0]12	[P][OP]22	MÓNICA CAMPOVERDE	ADMISIONES	ADMISION	0	3	3	3
[L][BUILDING][PISO0]13	[P][OP]22	MÓNICA CAMPOVERDE	ECONOMA1	NUTRICION	0	3	3	3
[L][BUILDING][PISO0]14	[P][OP]23	ELIZABETH AGUIRRE	COCINA_BAR	EMERGENCIA	0	3	3	3

ID EDIFICACION	Código Empleado	Empleado	Nombre Equipo	Departamento	Planta	Confidencialidad	Disponibilidad	Integridad
[L][BUILDING][PISO5]18	[P][OP]23	ELIZABETH AGUIRRE	DIRMEDICA	DIRECCION MEDICA	5	3	3	3
[L][BUILDING][PISO1]4	[P][OP]24	MA. EUGENIA PLAZA	NEONATOLOGIA	CUIDADOS INTENSIVOS	1	3	3	3
[L][BUILDING][PISO0]15	[P][OP]24	MA. EUGENIA PLAZA	CARDIO	CARDIOSI	0	3	3	3
[L][BUILDING][PISO3]1	[P][OP]25	FERNABDA PIEDRA	ENFERMERIA 3	ENFERMERIA	3	3	3	3
[L][BUILDING][PISO5]19	[P][OP]25	FERNABDA PIEDRA	GERENCIA	GERENCIA	5	3	3	3
[L][BUILDING][PISO0]16	[P][OP]26	ANA CRISTINA ANDRADE	ATENCIONCLIENTE	ATENCION AL CLIENTE	0	3	3	3
[L][BUILDING][PISO0]17	[P][OP]26	ANA CRISTINA ANDRADE	CRAYOSX	DEPARTAMENTO DE IMAGENOLOGIA	0	3	3	3
[L][BUILDING][PISO1]5	[P][OP]27	ANGÉLICA ORELLANA	SUMCENTRAL	QUIRÓFANOS	1	3	3	3
[L][BUILDING][PISO4]1	[P][OP]27	ANGÉLICA ORELLANA	ENFERMERIA4DOS	ENFERMERIA		3	3	3
[L][BUILDING][PISO0]18	[P][OP]28	ANGÉLICA ORELLANA	ECOGRAFIA01	DEPARTAMENTO DE IMAGENOLOGIA	0	3	3	3
[L][BUILDING][PISO0]19	[P][OP]28	ANGÉLICA ORELLANA	CAJAIMAGENES	DEPARTAMENTO DE IMAGENOLOGIA	0	3	3	3
[L][BUILDING][PISO1]6	[P][OP]29	DR ANDRES MALO	PCAISLAMIENTO	CUIDADOS INTENSIVOS	1	3	3	3

ID EDIFICACION	Código Empleado	Empleado	Nombre Equipo	Departamento	Planta	Confidencialidad	Disponibilidad	Integridad
[L][BUILDING][PISO4]1 - [L][BUILDING][PISO3]1 - [L][BUILDING][PISO4]1 - [L][BUILDING][PISO2]1	[P][OP]29	DR ANDRES MALO	HOSPITALIZACIÓN	ENFERMERIA		3	3	3
[L][BUILDING][PISO1]7	[P][OP]30	MÓNICA CAMPOVERDE	UCI	CUIDADOS INTENSIVOS	1	3	3	3
[L][BUILDING][PISO5]20	[P][OP]30	MÓNICA CAMPOVERDE	SECREGERENCIA	GERENCIA		3	3	3
[L][BUILDING][PISO5]21	[P][OP]31	DR VASQUEZ	ZENTYAL PROXY 01	SISTEMAS		3	3	3
[L][BUILDING][PISO0]20	[P][OP]31	DR VASQUEZ	CARTERA_SEGUROS	TESORIA	0	3	3	3
[L][BUILDING][PISO0]21	[P][OP]32	ELIZABETH AGUIRRE	NVASVR	ADMISION	0	3	3	3
[L][BUILDING][PISO5]22	[P][OP]32	ELIZABETH AGUIRRE	0	GERENCIA		3	3	3
[L][BUILDING][PISO0]22	[P][OP]33	ING BRUNO LEDESMA	0	FARMACIA	0	3	3	3
[L][BUILDING][PISO1]8	[P][OP]33	ING BRUNO LEDESMA	0	QUIRÓFANOS	1	3	3	3

Matriz de Equipo Auxiliar

ID	DESCRIPCION	FECHA INSTALACION	ESTADO	OBSERVACIONES	UBICACIÓN
[AUX][POWER]1	ACOMETIDA ELECTRICA	98	BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO0]
[AUX][UPS]1	UPS1	2000	BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO5]5
[AUX][UPS]2	UPS	may-11	BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO5]5
[AUX][UPS]3	UPS	may-11	BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO5]5
[AUX][UPS]4	UPS	may-11	BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO5]5
[AUX][UPS]5	UPS	may-11	BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO5]5
[AUX][UPS]6	UPS6	mar-13	BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO5]5
[AUX][UPS]7	UPS7		BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO1]
[AUX][GEN]1	GENERADOR	1998	BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO0]
[AUX][AC]1	AIRE ACONDICIONADO	2011	BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO0]
[AUX][AC]2	AIRE ACONDICIONADO	2012	BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO0]
[AUX][CABLING]1	CABLEADO		BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO5]5
[AUX][CABLING]2	CABLEADO		BUENO	SIN ESTRUCTURA ADECUADA	[L][BUILDING][PISO0]
[AUX][ROBOT][TAPE]1	IMB ULTRIUM2		BUENO	OBSOLETO	[L][BUILDING][PISO5]5
[AUX][ROBOT][DISK]1	DISCO EXTERNO 2TB		BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO5]5
[AUX][ROBOT][DISK]2	DISCO EXTERNO 2TB		BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO5]5
[AUX][ROBOT][SAFE]1	CAJA FUERTE		BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO5]5

Matriz de Soportes de Información

ID	DESCRIPCION	ESTADO	OBSERVACIONES	UBICACIÓN
[SI][ELECTRONIC][TAPE]1	IBM ULTRIUM 1	BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO5]
[SI][ELECTRONIC][TAPE]2	IBM ULTRIUM 2	BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO5]
[SI][ELECTRONIC][TAPE]3	IBM ULTRIUM 3	BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO5]
[SI][ELECTRONIC][TAPE]4	IBM ULTRIUM 4	BUENO	SIN OBSERVACIONES	[L][BUILDING][PISO5]

Matriz de Servicios

ID	DESCRIPCION	ESTADO	OBSERVACIONES	UBICACIÓN
[S][WWW]	INTERNET	ACTIVO	SIN OBSERVACIONES	TODO
[S][APP]	SOFTWARE	ACTIVO	SIN OBSERVACIONES	TODO
[S][EMAIL]	CORREO ELECTRONICO	ACTIVO	SIN OBSERVACIONES	TODO

Matriz de Redes de Comunicación

ID	DESCRIPCION	ESTADO	OBSERVACIONES	UBICACIÓN
[COM][PSTN]1	RED TELEFONICA	ACTIVO	SIN OBSERVACIONES	TODO
[COM]RADIO]1	RED INALAMBRICA	ACTIVO	SIN OBSERVACIONES	TODO
[COM][LAN]1	RED LCCAL	ACTIVO	SIN OBSERVACIONES	TODO
[COM][INTERNET]1	INTERNET	ACTIVO	SIN OBSERVACIONES	TODO

Matriz de Recursos Humanos

ID RRHH	Cod Empleado	Empleado	TIPO ACTIVO
[P][UI]1	[P][OP]1	BELÉN PAREDES	OP
[P][UI]2	[P][OP]2	MA. EUGENIA PLAZA	OP
[P][UI]3	[P][OP]3	MA. ISABEL SOLORZANO	OP
[P][UI]4	[P][OP]4	LORENA ENDERICA	OP
[P][UI]5	[P][OP]5	TANIA SAVALA	OP
[P][UI]6	[P][OP]6	ALEJANDRA ESPINA	OP
[P][UI]7	[P][OP]7	LILENA MUÑOZ	OP
[P][UI]8	[P][OP]8	PAOLA CHICA	OP
[P][UI]9	[P][OP]9	DIANA SUAREZ	OP
[P][UI]10	[P][OP]10	JOHANA MOSQUERA	OP
[P][ADM]11	[P][OP]11	FERNANDA NIVICELA	ADM
[P][UI]11	[P][OP]12	FERNANDA PIEDRA	OP
[P][UI]12	[P][OP]13	LORENA PEÑA	OP
[P][UI]13	[P][OP]14	FANNY MONTERO	OP
[P][UI]14	[P][OP]15	LORENA PEÑA	OP
[P][UI]15	[P][OP]16	JUAN ALARCÓN	OP
[P][UI]16	[P][OP]17	ESTELA LEÓN	OP
[P][UI]17	[P][OP]17	VERÓNICA MARIDUEÑA	OP
[P][UI]18	[P][OP]18	LUIS MARIO TAMAYO	OP
[P][UI]19	[P][OP]18	LUIS MARIO TAMAYO	OP
[P][UI]20	[P][OP]19	ELIZABETH AGUIRRE	OP
[P][UI]21	[P][OP]19	ELIZABETH AGUIRRE	OP
[P][UI]22	[P][OP]20	ELIZABETH AGUIRRE	OP
[P][UI]23	[P][OP]20	ELIZABETH AGUIRRE	OP
[P][UI]24	[P][OP]21	ELIZABETH AGUIRRE	OP
[P][UI]25	[P][OP]21	ELIZABETH AGUIRRE	OP
[P][UI]26	[P][OP]22	MÓNICA CAMPOVERDE	OP
[P][UI]27	[P][OP]22	MÓNICA CAMPOVERDE	OP
[P][UI]28	[P][OP]23	ELIZABETH AGUIRRE	OP
[P][UI]29	[P][OP]23	ELIZABETH AGUIRRE	OP
[P][UI]30	[P][OP]24	MA. EUGENIA PLAZA	OP
[P][UI]31	[P][OP]24	MA. EUGENIA PLAZA	OP
[P][UI]32	[P][OP]25	FERNABDA PIEDRA	OP
[P][UI]33	[P][OP]25	FERNABDA PIEDRA	OP
[P][UI]34	[P][OP]26	ANA CRISTINA ANDRADE	OP

ID RRHH	Cod Empleado	Empleado	TIPO ACTIVO
[P][UI]35	[P][OP]26	ANA CRISTINA ANDRADE	OP
[P][UI]36	[P][OP]27	ANGÉLICA ORELLANA	OP
[P][UI]37	[P][OP]27	ANGÉLICA ORELLANA	OP
[P][UI]38	[P][OP]28	ANGÉLICA ORELLANA	OP
[P][UI]39	[P][OP]28	ANGÉLICA ORELLANA	OP
[P][UI]40	[P][OP]29	DR ANDRES MALO	OP
[P][UI]41	[P][OP]29	DR ANDRES MALO	OP
[P][UI]42	[P][OP]30	MÓNICA CAMPOVERDE	OP
[P][UI]43	[P][OP]30	MÓNICA CAMPOVERDE	OP
[P][UI]44	[P][OP]31	DR VASQUEZ	OP
[P][UI]45	[P][OP]31	DR VASQUEZ	OP
[P][UI]46	[P][OP]32	ELIZABETH AGUIRRE	OP
[P][UI]47	[P][OP]32	ELIZABETH AGUIRRE	OP
[P][UI]48	[P][OP]33	ING BRUNO LEDESMA	OP
[P][UI]49	[P][OP]33	ING BRUNO LEDESMA	OP

Anexo 3

PLAN DE PRUEBAS CONTRA INCENDIO

DESCRIPCION	CUMPLE	NO CUMPLE	TIEMPO ESPERADO	TIEMPO MEDIDO
Sonó la alerta con sirena				
Las personas asignadas deben desconectar las instalaciones generales en el siguiente orden: gas, electricidad y agua en caso de que el suministro sea independiente a la red general				
Guardar absoluto silencio.				
No correr bajo ninguna circunstancia.				
Evitar causar confusión (gritos, llamadas, etc.).				
No salir del área por su cuenta o por lugares no señalados en el Plan de Evaluación				
Siga las vías de evacuación, escaleras y puertas determinadas en los planos salvo que haya un cambio de orden por parte del Grupo Director				
Tomar los activos de información que haya identificado como más relevantes y proceda con la evacuación				
Mantenga la calma, domine el pánico, actúe con serenidad, pida auxilio				
Trate de extinguir el fuego, siempre que posea el elemento extintor adecuado y la salida asegurada. En caso de escapar, no corra, camine rápido y en fila, cerrando a su paso la mayor cantidad de puertas y ventanas.				
Antes de abrir puertas, tóquelas para comprobar si están calientas, puede haber fuego del otro lado, si es así busque otra salida.				
Se recomienda que exista una persona que se encargue de abrir las puertas de acceso/salida del edificio en caso de evacuación				

Use siempre las escaleras, ante la existencia de humo desplácese gateando, cubriéndose boca y nariz con máscaras anti humo, toallas o pañuelos mojados, en escaleras con humo descienda gateando de espalda.				
Tener un botiquín a mano				
El desalojo de cada planta debe hacerse ordenadamente desde el sótano hacia arriba				
	Tiempo total desde ser		**10 min**	

PLAN DE PRUEBA CONTRA TERREMOTO

DESCRIPCION	CUMPLE	NO CUMPLE	TIEMPO ESPERADO	TIEMPO MEDIDO
Sonó la alerta con sirena				
Las personas asignadas deben desconectar las instalaciones generales en el siguiente orden: gas, electricidad y agua en caso de que el suministro sea independiente a la red general				
Tomar los activos de información que sea posible				
Colocarse debajo de una mesa o escritorio y agarrarse de él.				
Si no hay una mesa o escritorio, cubrirse la cabeza con sus brazos y o pararse o ponerse en cuclillas ya sea debajo del marco de una puerta lo más pegado posible a un rincón de la casa o edificio.				
Alejarse de las ventanas y vidrios, y de objetos pesados (como libreros, armarios o calentadores) que puedan caerse con las sacudidas.				
Quédese dentro del edificio ya que mucha gente, al tratar de escapar, resulta herida cerca de las entradas de los edificios con materiales que caen.				
Se recomienda que haya una persona que se encargue de abrir las puertas de acceso/salida del edificio en caso de evacuación				

Vea si existe una forma alternativa de escape para cada uno de los departamentos y que pueda ser usada en caso de que el plan original no funcione. Todos los miembros deben saber dónde está la escalera por si llegan a necesitarla				
Marque en forma clara los lugares donde puede encontrar alimentos, agua, el botiquín y el extintor.				
Marque claramente dónde están las fuentes de energía eléctrica y las tomas de gas para que sean apagadas o cerradas en caso de emergencia				
Determine el lugar en el que todos deben reunirse después de una emergencia				
Tener un botiquín a mano				
El desalojo de cada planta debe hacerse ordenadamente desde el sótano hacia arriba				
	Tiempo total desde ser		**10 min**	

PLAN DE PRUEBAS CONTRA INUNDACIONES

DESCRIPCION	CUMPLE	NO CUMPLE	TIEMPO ESPERADO	TIEMPO MEDIDO
Sonó la alerta con sirena				
Las personas asignadas deben desconectar las instalaciones generales en el siguiente orden: gas, electricidad y agua en caso de que el suministro sea independiente a la red general				
Guardar absoluto silencio.				
No correr bajo ninguna circunstancia.				
Evitar causar confusión (gritos, llamadas, etc.).				
No salir del área por su cuenta o por lugares no señalados en el Plan de Evaluación				

Siga las vías de evacuación, escaleras y puertas determinadas en los planos salvo que haya un cambio de orden por parte del Grupo Director				
Tomar los activos de información que sea posible				
Mantenga la calma, domine el pánico, actúe con serenidad, pida auxilio				
Trate de extinguir el fuego, siempre que posea el elemento extintor adecuado y la salida asegurada. En caso de escapar, no corra, camine rápido y en fila, cerrando a su paso la mayor cantidad de puertas y ventanas.				
Antes de abrir puertas, tóquelas para comprobar si están calientas, puede haber fuego del otro lado, si es así busque otra salida.				
Se recomienda que haya una persona que se encargue de abrir las puertas de acceso/salida del edificio en caso de evacuación				
Use siempre las escaleras, ante la existencia de humo desplácese gateando, cubriéndose boca y nariz con máscaras anti humo, toallas o pañuelos mojados, en escaleras con humo descienda gateando de espalda.				
Tener un botiquín a mano				
El desalojo de cada planta debe hacerse ordenadamente desde el sótano hacia arriba				
	Tiempo esperado		**10 min**	

PLAN DE PRUEBAS CONTRA CORTO CIRCUITO

DESCRIPCION	CUMPLE	NO CUMPLE
Que las conexiones entre cables este correcto		
Que los cables no se encuentren pelados		
Que los cables no se encuentren		

cerca de agua		
Que los cables estén protegidos con una vaina retardarte de llama		
Revisar el amperaje de los cables		
Que todas las instalaciones se encuentren en cañerías metálicas		

PLAN DE PRUEBAS CONTRA GOTERAS

DESCRIPCION	CUMPLE	NO CUMPLE
Revisar la humedad en las paredes y el piso de la oficina		
Revisar la humedad en el techo de la oficina		
Revisar en caso de que exista un baño o tuberías sobre la oficina que estas se encuentren en buen estado		
En caso de que exista una terraza sobre la oficina revisar que esta tenga un buen desagüe para que el agua no se empoce y produzca goteras		

PLAN DE PRUEBAS CONTRA CONTROL DE ACCESO AL CENTRO DE CÓMPUTO

INSTALACIONES CENTRO DE CÓMPUTO

DESCRIPCION	CUMPLE	NO CUMPLE
La puerta permanece cerrada		
La cerradura de acceso biométrico funcione correctamente		
Se lleva el registro de ingreso de personal		
El personal autorizado es correcto		

PLAN DE PRUEBAS CONTRA SEÑALIZACION DE EMEGENCIA

DESCRIPCION	CUMPLE	NO CUMPLE	TIEMPO ESPERADO	TIEMPO MEDIDO
La altura de las señales es de 1.80 metros a 2.1 metros medidos desde el piso				
Las señales de salida de emergencia se encuentran en la parte superior del marco de la puerta de evacuación				
La señal de extintor está a una altura de 1.80 metros y el equipo a 1.50 metros				
No hay otro aviso cerca de la señal de seguridad ya que puede impedir la visibilidad				
El espacio donde este colocado el extintor esta libre				
Las fechas de caducidad de los equipos correcta				
Las señales foto luminosas se encuentran ubicadas correctamente				
Las capacitaciones se cumplen				

PLAN DE PRUEBAS SOBRE EL CONTROL DE ACCESO AL SISTEMA INFORMATICO

DESCRIPCION	CUMPLE	NO CUMPLE
El operador conoce las condiciones de confidencialidad y del uso correcto de a información		
Para la creación de un usuario se recibe la autorización antes de proceder a crear la cuenta		
Para la creación, modificación y eliminación de cuentas es responsable únicamente la persona asignada para este cargo		
Se lleva la bitácora de creación, modificación y eliminación correctamente		
Se crea una contraseña temporal para luego cambiarla		

PLAN DE PRUEBAS SOBRE EL CONTROL DE LA CONTRASEÑA

DESCRIPCION	CUMPLE	NO CUMPLE
Es confidencial		
La contraseña tiene al menos una letra mayúscula, un número, caracteres especiales y letras minúsculas		
Tiene mínimo de siete caracteres		
Es una contraseña anteriormente registrada		
Está basada en cosas personales como nombre, cedula, teléfono, fecha de nacimiento, etc.		
Se encuentren impresa , pegada en la pantalla o en cualquier lugar donde personas no autorizadas pueden ver		

DEL ACCESO AL CORREO ELECTRONICO

DESCRIPCION	CUMPLE	NO CUMPLE
Solo el personal tiene acceso al correo electrónico		
Solo se envían correos internos		
El correo basura está bloqueado		

DE ACCESO DE EQUIPOS ELECTRONICOS

DESCRIPCION	CUMPLE	NO CUMPLE
Se registra al personal en la entrada sus computadoras y medios de almacenamiento en el área de recepción.		

DE ACCESO REMOTO

DESCRIPCION	CUMPLE	NO CUMPLE
La dirección de sistemas es responsable de proporcionar el servicio de acceso remoto		
Para el acceso remoto de terceros se es autorizado por la gerencia		
Hay una persona responsable observando durante el acceso remoto		

DE ACCESO A LOS EQUIPOS DE CÓMPUTO

DESCRIPCION	CUMPLE	NO CUMPLE
Se piden los permisos necesarios al propietario de la información para acceder a la información		
Se accede al equipo de cómputo con la supervisión del propietario		
La información administrativa de uso restringido se encuentra cifrada		

PLAN DE PRUEBAS SOBRE BACKUPS DE EQUIPOS ADMINISTRATIVOS Y SERVIDORES

DESCRIPCION	CUMPLE	NO CUMPLE
Se realizan copias de respaldo o backups semanalmente y el último día del mes.		
Lo realizara el encargado de Sistemas		

DE EQUIPOS DEL PERSONAL

DESCRIPCION	CUMPLE	NO CUMPLE
la información generada diariamente esta almacenada en el disco duro c\:		
Semanalmente la información es respaldada en discos externos por el jefe se sistemas de acuerdo a un horario elaborado por el mismo		
Solo el personal autorizado puede utilizar Pen Drives - Memorias USB, discos externos, CD y DVD, para el manejo y traslado de información o realización de copias de seguridad		

TRASLADO

DESCRIPCION	CUMPLE	NO CUMPLE
Los Backups son trasladados a una oficina que se encuentre fuera del hospital a un rango de 3km a la redonda		
Las hojas de ruta se llevan correctamente		
Se definió al personal encargado de este proceso		
Se entregan los permisos de gerencia para que se realice el traslado		

PRUEBAS

DESCRIPCION	CUMPLE	NO CUMPLE
Mensualmente se hace simulacros de los backups al azar.		
Se registra una bitácora		

PLAN DE PRUEBAS SOBRE ESCRITORIO LIMPIO

DESCRIPCION	CUMPLE	NO CUMPLE
El sistema se cierra correctamente		
Los archivos utilizados se cerraron y guardaron correctamente		
El equipo y la pantalla fue cerrado correctamente		
Los documentos en papel se encuentran guardados en el cajón o estante correcto		
El escritorio se encuentra libre sin ningún documento		

PLAN DE PRUEBAS SOBRE HARDWARE ADQUISICIÓN

DESCRIPCION	CUMPLE	NO CUMPLE
Se realizó la solicitud la necesaria		
El Jefe de Sistemas y la gerencia analizaron la solicitud pasaron al personal de compras para que se realice la compra		
Una vez realizada la compra se la entrega al jefe inmediato del usuario		
El registro de todos los equipos del Hospital está correcto		

INSTALACION

DESCRIPCION	CUMPLE	NO CUMPLE
Los equipos no deben estar sobre alfombra deben estar levantados del piso		
Se comprobó la polaridad		
No deben estar cerca de ventanas o donde reciban mucho sol		
No deben haber elementos encima de los equipos		
No deben estar en lugares húmedos o cerca de tuberías		

PLAN DE PRUEBAS SOBRE LIMPIEZA Y MANTENIMIENTO DE LOS EQUIPOS

DESCRIPCION	CUMPLE	NO CUMPLE	TIEMPO ESPERADO	TIEMPO MEDIDO
Para limpiar se humedece una toalla pequeña y se limpiar la pantalla y el CPU con cuidado de no desconectar los cables				
No hay objetos encima del equipo de cómputo o que tapan las salidas de ventilación del CPU.				
No se come cerca del computador				
No se toma líquidos cerca del computador				
No se fuma				

SUMINISTROS ESCENCIALES

DESCRIPCION	CUMPLE	NO CUMPLE	TIEMPO ESPERADO	TIEMPO MEDIDO
Diariamente revisar la cantidad de papel				
Se realiza la solicitud con anticipación a inventarios				
Se toma en cuenta el aviso del equipo de que se está terminando en tóner de la impresora				
Se realiza la solicitud con anticipación a inventarios				

PLAN DE PRUEBAS SOBRE EL ROBO DE EQUIPOS

DESCRIPCION	CUMPLE	NO CUMPLE	TIEMPO ESPERADO	TIEMPO MEDIDO
Se realizó una denuncia dentro del Hospital				
El jefe de sistemas y de seguridad reviso la causa de la desaparición del equipo				
Si se comprobó robo se realizó la denuncia a la gerencia				
Se entregaron a tiempo los registros de salida del personal				
Se revisaron las cámaras de seguridad				
Se realizaron los tramites con la aseguradora				
Se retomó el trabajo en el menor tiempo posible				

PLAN DE PRUEBAS SOBRE SOFTWARE

ADQUISICION

DESCRIPCION	CUMPLE	NO CUMPLE	TIEMPO ESPERADO	TIEMPO MEDIDO
Se realizó la solicitud necesaria				
El Jefe de Sistemas y la dirección medica analizaron la solicitud				
Si se aprueba se pasa la solicitud al personal de compras para que se realice la compra				
El software comprado tiene licencias				
Si el software es libre se obtiene de sitios oficiales y seguros				
Se entregó al jefe de sistemas para que este realice la instalación en los equipos				

INSTALACIÓN

DESCRIPCION	CUMPLE	NO CUMPLE	TIEMPO ESPERADO	TIEMPO MEDIDO
Justifico su uso y pidió la autorización de instalación a su jefe inmediato.				
Solo se instalación software con licencias y de acuerdo a la propiedad intelectual.				
Para reinstalar un programa se borra completamente la versión instalada, para luego instalar la nueva versión.				
Las licencias se encuentran al día				
Todos los equipos cuentan con software de seguridad (antivirus, vacunas, privilegios de acceso , entre otros)				

TRASLADO

DESCRIPCION	CUMPLE	NO CUMPLE	TIEMPO ESPERADO	TIEMPO MEDIDO
El software solo puede ser trasladado al local fuera del mismo donde se encuentran los backups				
Internamente el software únicamente se traslada con la autorización y supervisión del jefe de sistemas				

BAJA DEL SOFTWARE

DESCRIPCION	CUMPLE	NO CUMPLE	TIEMPO ESPERADO	TIEMPO MEDIDO
Se realizó la solicitud al jefe inmediato para dar de baja al software que tenga en su computador y sea obsoleto				
Se realizó la solicitud al jefe de sistemas				
Se analizó el equipo para eliminar el software				
La desinstalación se guardó en la bitácora				

ACTUALIZACION

DESCRIPCION	CUMPLE	NO CUMPLE
se realizar de acuerdo a la calendarización		

PLAN DE PRUEBAS SOBRE ANTIVIRUS

INSTALACION

DESCRIPCION	CUMPLE	NO CUMPLE
Se revisa que no exista otro instalado en el equipo		
El antivirus cuenta con las licencias respectivas		

MANTENIMIENTO

DESCRIPCION	CUMPLE	NO CUMPLE
Se actualiza diariamente		
Se bloquean los dispositivos USB - CD ROM mediante el antivirus		
Se realizan limpiezas del equipo semanalmente		
Desde el servidor principal del antivirus se instalar y desinstalar la aplicación de todos los equipos		

PLAN DE PRUEBAS SOBRE REDES DE COMUNICACIÓN

INTERNET

DESCRIPCION	CUMPLE	NO CUMPLE
El internet esta restringido para actividades del trabajo		
Las páginas y palabras no permitidas están bloqueadas y esto esta registrado correctamente		
Se monitorea a los usuarios de internet aleatoriamente acerca de sus actividades		
No está permitido descargar software sin autorización		
Se controla el uso de internet para juegos y diversión		

TELEFONO FAX Y CORREO

DESCRIPCION	CUMPLE	NO CUMPLE
Solo se usan para actividades de trabajo.		
Se controla el uso personal estos medios ya que ocasional está permitido		

Anexo 4

Procesos del Hospital Santa Inés

ID	PROCESOS
1.	**Quirófano**
1.2	**Gestión Quirófano**
1.2.1	Descargos de insumos y medicamentos
1.2.2	Funcionamiento de equipos de Quirófano
1.3	**Atención Médica (Qx)**
1.3.1	*Estado Hemodinámico del paciente durante la intervención quirúrgica
1.4	**Atención Enfermería (Qx)**
1.4.1	*Descargo de derechos del paciente de uso de equipos especiales
1.4.2	*Descargo de insumos y materiales utilizados en la cirugía
1.4.3	*Conformidad del instrumental e insumos entregados para la cirugía
1.5	**Salas de Cirugías**
1.5.1	*Administración de medicamentos
1.6	**Recuperación**
1.6.1	*Inventario del stock de insumos y medicamentos
1.6.2	*Signos vitales
1.6.3	*Recuperación del paciente luego de la intervención quirúrgica
1.7	**Suministro Central**
1.7.1	*Esterilización de equipos y materiales
2.	**Intervención**
2.1	**Administración - CARDIOSI**
2.1.1	*Oportuno abastecimiento de insumos, medicamentos y dispositivos
2.1.2	*Archivo de documentación generada para el abastecimiento
2.1.3	*Seguimiento de aprobación a las proformas por convenios
2.1.4	*Existencias físicas vs. registros contables de dispositivos, insumos y medicamentos.
2.2	**Atención Médica y Enfermería - CARDIOSI**
2.2.1	*Estado y funcionamiento del angiografía y equipos del área
2.3	**Intervención - CARDIOSI**
2.3.1	*Eficacia y seguridad del procedimiento realizado
2.3.2	*Calidad de dispositivos médicos
2.3.3	*Calidad de obtención y procesamiento de las imágenes
2.4	**Intervención Endoscopías**
2.4.1	*Calidad de la imagen (balances de blancos)
2.4.2	*Pacientes de alto riesgo
2.4.3	*Calidad de exámenes (rutinas)
2.4.4	*Funcionamiento de los equipos
2.5	**Radiología Intervencionista**
2.5.1	*Procedimientos médicos

2.5.2 *Disponibilidad de materiales
2.6 **Curaciones e Intervenciones Menores**
2.6.1 *Correcta emisión del Expediente Médico
3. **Hospitalización**
3.1 **Gestión de Hospitalización**
3.1.1 *Mantenimiento preventivo de bombas infusión (servicio externo)
3.1.2 *Turnos de personal
3.2 **Atención Médica (H)**
2.2.1 *Evolución del estado del paciente durante su hospitalización
3.3 **Atención Enfermería (H)**
3.3.1 *Stock de Subbodegas
3.3.2 *Stock y fechas de expiración del Carro de Paro
3.3.3 *Inventario de Control remoto de televisiones en habitaciones
3.3.4 *Inventario de Equipos de enfermería
3.4 **Ingreso y Salida de Pacientes por Hospitalización**
3.4.1 *Alta del paciente
4. **Fianzas**
4.1 **Tesorería**
4.1.1. *Cartera
4.1.2. *Pagos por transferencia
4.2 **Caja Médica**
4.2.1 *Descuentos y pagos mensuales de médicos
4.3 **Pagaduría**
4.3.1 *Cumplimiento de plazos de pagos por proveedor
4.4 **Jefatura de Caja**
4.4.1 *Facturación de cuentas pendientes
4.4.2 *Cuadres de caja
4.5 **Caja**
4.5.1 *Datos llenados correctamente para su facturación
5. **Farmacia**
5.1 **Gestión de Farmacia**
5.1.1 Cuadre de dinero y facturación correcta
5.1.2 Egresos por transferencias a subbodegas y bodegas
5.1.3 Stock de Psicotrópicos y Estupefacientes
5.1.4 Personal
5.1.5 Fechas de caducidad
5.2 **Compras**
5.2.1 *Devolución de Productos
5.2.2 *Almacenamiento e Identificación de Medicamentos e Insumos
5.2.3 *Conformidad de pedidos
5.3 **Dispensación Externa**
5.3.1 Correcta dispensación de la receta
5.4 **Dispensación Interna**

5.4.1 Correcta dispensación de la receta

6. **Laboratorio**

6.1 **Exámenes de Laboratorio**

6.1.1 *Identificación de muestras

6.1.2 *Limpieza de equipos

6.1.3 *Resultados de exámenes

6.1.4 *Stock de reactivos y materiales

6.1.5 *Mantenimiento técnico preventivo (externo)

6.2 **Contabilidad de Laboratorio**

6.2.1 *Ingresos y Gastos

6.2.2 *Existencias físicas vs. Contable

6.2.3 *Asistencia del Personal y Horas extras

7. **Imagenología**

7.1 **Exámenes de Imagenología**

7.1.1 *Calidad de imágenes

7.1.2 *Funcionamiento de equipos

7.2 **Administración de Imagenología**

7.2.1 *Stock de insumos para Rayos X y Tomografía

8. **EXAMENES - CARDIOSI**

9. **CEDICARDIO**

9.1 Exámenes CEDICARDIO

9.2 Administración CEDICARDIO

9.2.1 *Financiero, contable y administrativo

10. **EXAMENES - ENDOSCOPÍASGASTROINTESTINAL**

10.1 *Calidad de la imagen (balances de blancos)

10.2 *Pacientes de alto riesgo

10.3 *Calidad de exámenes (rutinas)

10.4 *Funcionamiento de los equipos

11. **Emergencia**

11.1 **Gestión de Emergencia**

11.1.1 *Manejo emergente del paciente crítico

11.2 **Atención de Emergencia**

11.2.1 *Tamizaje de pacientes

11.3 **Atención Médica (E)**

11.3.1 *Correcto llenado de fichas y formularios

11.3.2 *Tamizaje de pacientes

11.4 **Atención Enfermería (E)**

11.4.1 *Inventario de subbodegas

11.4.2 *Administración de medicación

11.4.3 *Asignación de habitación

11.4.4 *Alta de pacientes

11.5 **Admisión Emergencia**

11.5.1 *Altas de los pacientes

12. **Convenios**

12.1 **Gestión de Convenios**

12.1.1 *Valores Planillados y/o Facturados por Convenios

12.1.2 *Consolidación de saldos con convenios

12.1.3 *Ingresos de pacientes por transferencia, emergencias y convenios

12.2 **Seguros del Estado**

12.2.1 *Información para la tramitación del SOAT y FONSAT

13. **Contabilidad**

13.1 **Estados Financieros**

13.1.1 *Ingresos y Gastos

13.1.2 *Correcta emisión de la documentación previa a la elaboración de comprobantes de pago

13.1.3 *Bancos

13.2 **Cuadre de Caja**

13.2.1 *Cuadre de Recaudaciones

13.3 **Comprobantes de Pago**

13.3.1 *Correcta emisión de la documentación previa a la elaboración de comprobantes de pago

13.4 **Roles de Pago**

13.4.1 *Horas Extras

13.4.2 *Descuentos de roles a crédito

14. **Compras**

14.1 *Asignación de bienes adquiridos

15. **Talento Humano**

15.1 **Gestión Talento Humano**

15.1.1 *Vacaciones y permisos

15.1.2 *Entradas y salidas (Marcaciones de personal)

15.1.3 *Capacidad de endeudamiento (préstamos)

15.2 **Manejo del Personal**

15.2.1 *Imagen de personal

15.2.2 *Ambiente de trabajo - Clima laboral

15.2.3 Capacitación y Formación

15.2.4 *Efectividad de las capacitaciones

16. **Planificación Estratégica**

16.1 **Planificación Estratégica**

16.1.1 *Cumplimiento de indicadores de la Planeación Estratégica

16.1.2 *Cumplimiento de proyectos

16.2 **Gestión de Calidad**

16.2.1 * Eficacia de acciones preventivas y correctivas

17. **Mercadeo y Comunicación**

17.1 **Gestión de Mercadeo**

17.1.1 *Cumplimiento de pautajes comprados

17.1.2 *Calidad y diseño de imágenes

17.2 **Comunicación Interna**

17.2.1 *Actualización de carteleras de información

17.3 **Comunicación Externa**

17.4 **RRPP**

17.4.1 *Ejecución del proceso de posicionamiento a través de los medios

18. **Dirección Medica**

18.1 **Gestión de Dirección Médica**

18.1.1 *Cumplimiento de la asignación de turnos de médicos residentes

18.1.2 *Correcta y completa emisión del expediente médico (control aleatorio)

18.2 **Jefatura de Residentes**

18.2.1 *Cumplimiento del trabajo asignado a médicos residentes

18.3 **Jefatura de Enfermeras**

18.3.1 *Turnos y vacaciones

18.3.2 *Cumplimiento del trabajo asignado a las enfermeras de acuerdo a los turnos

18.3.3 *Funcionamiento e inventario de equipos en Quirófano, UCI, Emergencia, Hospitalización

18.3.4 *Disponibilidad del carro de paro y/o vitrinas en los lugares asignados

18.4 **Gestión de Auditoría Médica**

18.4.1 *Correcto levantamiento de la documentación del expediente médico (control aleatorio)

18.5 **Comité de Calificación y Auditoría Médica**

18.5.1 *Idoneidad de la documentación de cada especialista que solicita trabajar en el hospital.

18.6 **Comité Técnico**

18.7 **Departamentos Médicos**

19. **Alta dirección**

19.1 **Junta General**

19.1.1 *Estados financieros y cumplimiento de derechos, atribuciones y obligaciones establecidas en los estatutos y los de ley

19.2 **Directorio**

19.2.1 *Estados Financieros, presupuestos y proyectos

19.2.2 *Políticas Administrativas

19.2.3 *Políticas Asistenciales

19.3 **Presidencia**

19.3.1 *Estados Financieros, presupuestos y proyectos

19.3.2 *Políticas Administrativas

19.3.3 *Políticas Asistenciales

19.4 **Gerencia**

19.4.1 *Estados Financieros, presupuestos y proyectos

19.4.2 *Políticas Administrativas

19.4.3 *Políticas Asistenciales

19.5 **Asistencia de Alta Dirección**

19.5.1 *Planillajes y Facturación de arriendos

20. **Nutrición**

20.1 **Gestión de Nutrición**
20.1.1 *Cantidad de comidas servidas al personal
20.2 **Compras de Nutrición**
20.2.1 *Ingresos y Egresos de alimentos
20.3 **Dietas**
20.3.1 *Cantidad y tipo de dietas servidas al paciente
21. **Sistemas**
21.1 Implementar soluciones
21.2 Soporte técnico
21.3 Proveer servicios informáticos

Anexo 5

HOSPITAL SANTA INES

FORMATO DE CREACION DE NUEVAS CUENTAS

(RRH-PCC-001)

CREACION		MODIFICACION		BAJA TEMPORAL		BAJA DEFINITIVA	

No.	Nombres y Apellidos Usuario	Departamento	ID Usuario	Observaciones

HOJA DE RUTA PARA EL TRASLADO DE BACKUPS

(PSB-STB-001)

Cedula	Nombre	Fecha – Hora	Entrega	Firma receptor	Firma emisor	Observaciones

HOSPITAL SANTA INES

INSTALACION DE SOFTWARE

(SAS-SOF-001)

Cedula	Nombre	Departamento	Software	Tiempo requerido	Firma	Observaciones

HOSPITAL SANTA INES				**CREACION, MODIFICACION DE USUARIOS** (RRH-ALT-001)	
INFORMACION PERSONAL					
Cedula				**Fecha**	
Nombres				**Apellidos**	
Telefono				**Celular**	
Fecha Nacimiento	**Dia**	**Mes**	**Año**	**Email**	
INFORMACION DE LA CLINICA					
Departamento					
Cargo					
Información electrónica disponible					
	Historial de la clínica				
	Contabilidad				
	Financiero				
	Enfermería				
	Activos Fijos				
	Economato				
	Caja Medica				
	Facturación				
	Hospitalización				
	Emergencia				
	Bancos				
	Botica				
	Quirófano				
Servicios adicionales					
	Internet				
	Mail				
	Extensión telefónica				
Observaciones					

_____ _____

Firma Usuario Firma Gerente General

HOSPITAL SANTA INES	**CONTROL DE ACCESO A AREAS RESTRINGUIDAS** (SEG-ACT-001)		
Informacion			
Cedula		**Fecha**	
Nombres y Apellidos			
Departamento		**Cargo**	
Razones de ingreso			

HOSPITAL SANTA INES	**PRUEBA DE RESPALDOS** (PEB-PMB-001)		
Información			
Nombre de respaldo		**Fecha**	
Nombre responsable			
Departamento			
Observaciones de la prueba			

REUBICACION INTERNA DE EQUIPO
(RDE-MEC-001)

INFORMACION DE USUARIO			
ID/Cedula		**Fecha**	
Nombre y Apellido			
Telefono		**Celular**	
Deparatmento		**Cargo**	
DATOS DE EQUIPO			
Equipo		**IP**	
Serial			
Programas importantes			
Ubicación información importante			
INFORMACION PERSONA QUE RETIRA EL EQUIPO			
ID/Cedula		**Fecha**	
Nombre y Apellido			
Telefono		**Celular**	
Deparatmento		**Cargo**	
Observacion previa			

_____ _____ _____

Firma Usuario **Firma Responsable** **Firma Gerente Genera**

INFORME DE DAÑO DE EQUIPO
(SAS-SOF-002)

INFORMACION DE USUARIO			
ID/Cedula		**Fecha**	
Nombre y Apellido			
Telefono		**Celular**	
Deparatmento		**Cargo**	
DATOS DE EQUIPO			
Equipo		**IP**	
Serial			
Programas importantes			
Ubicación información importante			
BREVE DESCRIPCION SOBRE EL DAÑO			

_____ _____ _____

Firma Usuario **Firma Responsable** **Firma Gerente General**

HOSPITAL SANTA INES

REGISTRO DE PERSONAL INGRESO A CENTRO DE COMPUTO

(PCA-PIC-001)

ID	NOBRES Y APELLIDOS	TELEFONO	PERSONA QUE AUTORIZO	FIRMA	OBSERVACIONES

HOSPITAL SANTA INES

REGISTRO DE BACKUPS SEMANALES DEL PERSONAL

(PCB-PEB-001)

ID	CEDULA	NOMBRE	ENCARGADO	FIRMA EMPLEADO	FIRMA ENCARGADO	OBSERVACIONES

HOSPITAL SANTA INES

REGISTRO DE ABASTECIMIENTO DE SUMINISTROS

(ISE-RHP-001)

CEDULA	NOMBRE	DEPARTAMENTO	SUMINISTRO	FIRMA EMISOR	FIRMA RECEPTOR	FECHA

HOSPITAL SANTA INES

RESPONSABLES DE LOS EQUIPOS

(SCS-SME-001)

FECHA	RESPONSABLE	DEPARTAMENTO	NOMBRE EQUIPO	SERIAL	FIRMA RESPONSABLE

SOLICITUD DE ADQUISICION, REPARACION, ACTUALIZACION MANTENIMIENTO O CAMBIO DE MATERIALES Y EQUIPOS

(SAH-HAR-001)

Fecha Solicitud	**Día**	**Mes**	**Año**	**Tipo Solicitud**	**Adquisición**	**Revisión**
					Actualización	**Cambio**
					Mantenimiento	**Otro**
Solicitante			**Cargo**		**Departamento**	

Tipo				**Datos Equipo**	
Equipo		**Herramienta**		**Marca**	
Materiales		**Papelería**		**Modelo**	
Insumos		**Aseo**		**Serie**	
Otro		**Software**		**No de Inventario**	
Cuál?				**Ubicación**	
				Responsable	

Descripción de la razón de la solicitud				
Fecha de recibo de solicitud	**Día**	**Mes**	**Año**	

_____ _____

Firma Usuario **Firma Responsable**

CREACION, MODIFICACION DE USUARIOS

(EDI-CPD-EDG-001)

INFORMACION PERSONAL					
Cedula				**Fecha**	
Nombres				**Apellidos**	
Telefono				**Celular**	
Fecha Nacimiento	**Dia**	**Mes**	**Año**	**Email**	
INFORMACION DE LA CLINICA					
Departamento					
Cargo					
Información electrónica disponible					
	Historial de la clínica				
	Contabilidad				
	Financiero				
	Enfermería				
	Activos Fijos				
	Economato				
	Caja Medica				
	Facturación				
	Hospitalización				
	Emergencia				
	Bancos				
	Botica				
	Quirófano				
Servicios adicionales					
	Internet				
	Mail				
	Extensión telefónica				
Observaciones					

INFORME DE ESCRITORIO LIMPIO

(SEC-SME-001)

INFORMACION DE USUARIO			
ID/Cedula		**Fecha**	
Nombre y Apellido			
Telefono		**Celular**	
Deparatmento		**Cargo**	

OBSERVACIONES	**SI**	**NO**
El equipo está apagado		
Hay documentos sobre el escritorio		
Hay basura sobre el escritorio		
Los documentos importantes se encuentran en el lugar indicado		
Hay objetos sobre el equipo informático		
Los cables del equipo se encuentran colocados correctamente		
La impresora se encuentra apagada		
Los dispositivos de almacenamiento en caso de tener se encuentran guardados en un lugar seguro		

Observaciones	

_____ _____

Firma Usuario **Firma Responsable**

HOSPITAL SANTA INES

ENTREGA DE EQUIPOS
(SAH-HAR-002)

INFORMACION DE PERSONA QUE ENTREGA			
ID/Cedula		**Fecha**	
Nombre y Apellido			
Departamento		**Cargo**	
DATOS DE EQUIPO			
Equipo		**IP**	
Serial			
Programas instalados			
INFORMACION PERSONA RECIBE			
ID/Cedula		**Fecha**	
Nombre y Apellido			
Departamento		**Cargo**	

_____ _____

Firma Usuario **Firma Responsable**

HORARIO MANTENIMIENTO DE LOS EQUIPOS

(ADE-MLP-001)

FECHA	ENCARGADO	DEPARTAMENTO	TIEMPO ESTIMADO

_____

Firma Responsable

_____

Firma Gerente General

BITACORA DE PAGINAS Y PALABRAS BLOQUEADAS EN INTERNET

(RDC-UDI-001)

FECHA	PAGINA	FECHA	PALABRAS

Anexo 6

Diseño de Tesis

UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACION

ESCUELA DE INGENIERÍA DE SISTEMAS

DISEÑO DE TESIS

TEMA

“Políticas de Seguridad de la Información aplicadas al Hospital Santa Inés”

DIRECTOR

ING. ESTEBAN CRESPO

AUTOR

DANIELA CALDERON GOERCKE

2012

INDICE

1. Título del proyecto

"Políticas de Seguridad de la Información aplicadas al Hospital Santa Inés"

2. Selección y delimitación del tema

La seguridad de la Información en la actualidad se ha convertido en una de las partes más importantes de las empresas ya que con esta protegemos la información de las amenazas que se podrían presentar como: ser divulgada, mal utilizada, robada, borrada, etc. Con estos argumentos surge la propuesta de realizar un estudio completo y actual de la Seguridad de la Información del Hospital Santa Inés, con el cual se brindará un manual con Políticas de Seguridad de la misma.

Para el desarrollo de estas políticas se investigará acerca de los activos de la información y las amenazas que podrían poner en riego, teniendo riesgos tanto ambientales, lógicos, humanos y de telecomunicaciones. Para luego clasificar estos activos y ponderar riesgos e impactos.

3. Descripción del objetivo de estudio

El objetivo principal de esta investigación es ayudar a prevenir las amenazas que existen, las cuales podrían poner en riesgo la información privada que maneja el Hospital Santa Inés.

Se proveerán medidas para mantener los riesgos bajo control y así conservar la integridad, disponibilidad, autenticidad de la información del Hospital. Para esto se necesitará la colaboración del personal del Hospital, realizando una investigación sobre todos los activos de información y las amenazas para la institución en mención.

Como resultado de esta investigación se entregará un manual con Políticas de Seguridad que deberá tenerse en cuenta dentro del Hospital. Estas estrategias serán presentadas de manera clara y sencilla para que el personal pueda entenderlas, aplicarlas, ejecutarlas monitorearlas y controlarlas.

4. Resumen del Proyecto

Lo que se pretende realizar es un levantamiento de la información con un análisis y gestión de riesgos de la seguridad de la información del hospital Santa Inés mediante técnicas de muestreo, encuestas y observación. Quedando como resultado un manual de Políticas de Seguridad de la Información que ayudarán a proteger la misma.

Investigación

La investigación se desarrollará en tres fases en la primera se investigará los activos de la información y las posibles amenazas del Hospital Santa Inés. Los activos de la información serán analizados en cuatro niveles: ambientales, de recursos humanos, lógicos y de telecomunicaciones, relacionados con los servicios que brinda el Hospital.

En la segunda fase se clasificarán los activos y se realizará un análisis de los riegos e impactos de las amenazas que podrían suceder.

Finalmente en la tercera fase se desarrollarán las Políticas de Seguridad de la Información.

5. Introducción

Planteamiento del problema

El propósito de la creación de Políticas de Seguridad de la Información para el Hospital Santa Inés, es desarrollar un estudio completo del estado actual y futuro de su seguridad informática, brindando un plan estratégico, que si bien no brinda la solución total, podría cubrir una gran parte del problema.

La mayoría de personas que manejan la información desconocen el gran problema que podría provocar el daño o pérdida de esta, y no invierten ni capital humano ni económico para prevenirlo. El objetivo principal de la seguridad informática es mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información.

Justificación e impactos

La seguridad informática es básica para cualquier tipo de empresa u organización, pero ¿De quién debemos protegernos? Se llama intruso a la persona que accede sin autorización a nuestro sistema, ya sea de forma intencional o no, y se clasifican según su nivel de conocimiento. Pero los intrusos no son los únicos peligros, también están los desastres naturales, como un terremoto o incendio, los daños en telecomunicaciones, en las redes internas, entre otros.

Por esto es importante proteger los tres elementos básicos que son el hardware, software y los datos, siendo el más importante el último ya que si existiera un daño en el hardware o software, estos pueden adquirirse nuevamente; pero los datos obtenidos con el transcurso del tiempo son imposibles de recuperar.

Las amenazas y ataques se pueden clasificar como ataques pasivos, en donde el atacante no altera la comunicación, sino solo escucha o monitoriza para obtener la información que está siendo transmitida; y ataques activos, donde el atacante modifica de alguna manera el flujo de datos.

Por todos estos daños se pretende realizar un manual con Políticas de Seguridad y tratar de mitigar todos los posibles riesgos y amenazas que podrían afectar a los activos de información, ya sea en este momento o en el futuro.

Objetivo General
Desarrollo de Políticas de Seguridad de la Información aplicadas al Hospital Santa Inés, para mitigar los impactos originados por los posibles riesgos.

Objetivos Específicos
Para llegar al objetivo general señalado serán necesarios objetivos específicos como los siguientes:

- Aplicar la Metodología de Análisis de la Gestión de Riesgos de los Sistemas de Información (MAGERIT)
- Aplicar los componentes de la Norma ISO 27001 aplicada a la gestión de Seguridad de la Información
- Levantar los activos de la Información y las posibles amenazas ambientales, lógicas, de recursos humanos y telecomunicaciones relacionadas con los servicios que brinda el Hospital Santa Inés.
- Clasificar los activos de información y las amenazas. Ponderar riegos y probabilidades de impactos
- Desarrollar las Políticas de Seguridad de la Información para el Hospital Santa Inés.
- Realizar las recomendaciones pertinentes sobre tema seguridad de información al personal administrativo del hospital.

6. Marco Teórico

• Seguridad de la Información

La seguridad de la información son todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología, la información es poder. Se clasifica como:

Crítica: Es indispensable para la operación de la empresa.

Valiosa: Es un activo de la empresa y muy valioso.

Sensible: Debe de ser conocida por las personas autorizadas

- ## MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgos de la Seguridad de Información) fue elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

Esta metodología es interesante para todos quienes trabajan con información digital y sistemas informáticos. Si esta información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es importantísimo para poder gestionarlos.

MAGERIT persigue los siguientes objetivos:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

- ## ACTIVOS DE INFORMACION Y AMENAZAS

Activos son los recursos del sistema de información necesarios para que la organización funcione correctamente y alcance los objetivos propuestos. Los activos más importantes son:

  - Los servicios

- Las aplicaciones informáticas (software)
- Los equipos informáticos (hardware)
- Los soportes de información (dispositivos de almacenamiento de datos)
- Equipamiento auxiliar
- Las redes de comunicación (el intercambio de datos)
- Las instalaciones
- Las personas

A estos activos se les debe clasificar según su especie, para luego darles una valoración, no de lo que cuesta en dinero sino de cuánto vale dentro de la organización.

Las amenazas son las cosas que pueden afectar a cada activo, son cosas que ocurren y pueden dañar a los activos. Pueden ser accidentes naturales (terremotos, inundaciones), desastres industriales (contaminación), amenazas causadas por personas como errores o ataques intencionados.

Cuando un activo es víctima de una amenaza se debe estimar cuan vulnerable es, en dos sentidos:

- Degradación: mide el daño causado por un incidente en el supuesto de que ocurriera.
- Frecuencia: cada cuanto se materializa la amenaza.

• RIESGO E IMPACTO

El impacto es la medida del daño sobre el activo derivado de la materialización de una amenaza. Hay dos tipos de impactos:

- Impacto acumulado: calculado sobre el activo , teniendo en cuenta su valor acumulado y las amenazas a las que está expuesto
- Impacto repercutido: calculado sobre un activo teniendo en cuenta su valor propio y las amenazas a las que están expuestos los activos de los que depende.

El riesgo es la medida del daño probable sobre un sistema. El riesgo crece con el impacto y con la frecuencia.

- Riesgo acumulado: calculado sobre un activo teniendo en cuenta el impacto acumulado sobre un activo debido a una amenaza y la frecuencia de la amenaza.
- Riesgo repercutido: calculado sobre un activo teniendo en cuenta el impacto repercutido sobre un activo debido a una amenaza y la frecuencia de la misma.

- **ISO 27001**

  ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) es un estándar internacional para la seguridad de la información que fue aprobado y publicado en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

  ISO/IEC 27001 es la única norma internacional auditable que define los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI). La norma fue creada para garantizar una selección de controles de seguridad adecuados y proporcionales.

  Aquí se especifican los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI según el conocido "Ciclo de Deming" o PDCA, que es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart. Las siglas PDCA son el acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

  Todo esto nos ayuda a proteger los activos de información y dar mayor confianza a cualquiera de las partes interesadas, sobre todo a los clientes. ISO/IEC 27001 es una norma adecuada para cualquier organización, grande o pequeña, de cualquier sector o parte del mundo.

7. Metodología

Tipo de Estudio

La clase de investigación a realizar será en gran parte evaluativa y experimental, ya que lo primero que se hará es una valoración de los activos y amenazas de la información, para luego realizar un análisis sobre las mismas y finalmente crear las políticas de seguridad.

Método

Para la recopilación de información nos basaremos en:

- Libros: Permitirá obtener conocimientos proporcionados por autores a través de sus publicaciones, lo cual nos servirá para el desarrollo de nuestro proyecto.

- Entrevista y encuestas: Permitirá conocer en base a experiencias del personal los activos y amenazas.

- Internet: A través de este medio se conocerán los últimos avances tecnológicos y más información actualizada relacionadas con el tema.

Técnica e instrumento

Se utilizarán técnicas de observación, encuesta y entrevista, ya sea una guía de observación o un cuestionario con preguntas cerradas y abiertas, para indagar toda la información posible.

8. Contenidos

- **Introducción**
- **Objetivos**
- **Capítulo 1**
    - Que es Seguridad de la Información
    - Principios de la Seguridad de la Información
    - Importancia de la Seguridad de la Información
    - Tretas y Vulnerabilidades de la Seguridad de la Información
        - Ataques
        - Brechas de seguridad
        - Exposiciones
    - Elementos de Seguridad de la Información
        - Responsabilidad
        - Reusabilidad
        - Triangulo de seguridad, funcionabilidad y facilidad de uso
    - Revisión macro ISO 27001
    - MAGERIT
    - Clasificación y control de activos de seguridad
    - Políticas, planes y procedimientos de seguridad
    - Importancia del factor humano
    - Gestión de incidentes de seguridad
    - Gestión de continuidad del negocio

- **Capítulo 2**
    - Análisis de la situación real de la Seguridad de la Información del Hospital Santa Inés
        - Hardware
        - Software
        - Comunicaciones
        - Recursos humanos

- **Capítulo 3**
  - Levantamiento de activos de la información
    - Activos Hardware
    - Activos Software
    - Activos de Información electrónica
    - Activos de equipamiento
    - Activos de personal
    - Activos de medios de respaldo
    - Activos de Servicios
    - Activos de documentos de papel
  - Identificación de procesos del negocio
  - Clasificación de niveles de confidencialidad de cada activo
  - Clasificación de la disponibilidad de la información
  - Clasificación por niveles de los activos
  - Identificación de las amenazas, riesgos y probabilidades de impacto

- **Capítulo 4**
  - Elaboración de las Políticas de Seguridad de la Información de Hardware
    - Definición de las políticas
    - Procedimientos
    - Tareas
  - Elaboración de las Políticas de Seguridad de la Información de Software
    - Definición de las políticas
    - Procedimientos
    - Tareas
  - Elaboración de las Políticas de Seguridad de la Información Electrónica
    - Definición de las políticas
    - Procedimientos
    - Tareas
  - Elaboración de las Políticas de Seguridad de la Información de Equipamiento
    - Definición de las políticas
    - Procedimientos
    - Tareas
  - Elaboración de las Políticas de Seguridad de la Información de Personal
    - Definición de las políticas
    - Procedimientos
    - Tareas
  - Elaboración de las Políticas de Seguridad de la Información de Medios de respaldo

        - Definición de las políticas
        - Procedimientos
        - Tareas
    - Elaboración de las Políticas de Seguridad de la Información de los documentos en papel
        - Definición de las políticas
        - Procedimientos
        - Tareas
    - Elaboración de las Políticas de Seguridad de la Información de los Servicios
        - Definición de las políticas
        - Procedimientos
        - Tareas

- **Capítulo 5**
    - Objetivos
    - Tiempos de respuesta
    - Plan de capacitación
    - Plan de pruebas
    - Plan de control y retroalimentación

- **Capítulo 6**
    - Análisis de costo beneficio

- **Conclusiones y Recomendaciones**
- **Bibliografía**
- **Anexos**

9. Presupuesto

Gastos Fijos

• Computador portátil	$700	
	TOTAL	*$700*

Gastos Variables

• Internet de alta velocidad(6 Meses)	$300	
• Transporte	$45	
	TOTAL	*$345*

10. Referencias

Se ha visto la necesidad de tener como fuente de consulta principal el internet y algunos libros, para encontrar la información requerida.

Libros:

- Andrew S. Tanenbaum, Redes de Computadoras - Tercera edición, Prentice Hall
- Michael J. Donahoo, Kenneth L. Calvert, 2009, TCP/IP Sockets in C: Practical Guide for Programmers second edition, Morgan Kaufmann
- STALLINGS William, 2000, Comunicaciones y redes de computadores; Traducción: Juan Manuel López Soler, Pedro García Teodoro y José Luis Pérez Córdoba, Prentice Hall Año Publicación
- GOMEZ, Álvaro; 2008; "Enciclopedia de la Seguridad Informática"; (Spanish Edition)"; Alfaomega - Ra-Ma
- Barba Martí Antoni, 1999; Gestión de Red, Ediciones de la Universidad Politécnica de Cataluña
- HUIDROBO MOYA José, ROLDAN MARTINEZ David, Comunicaciones en redes WLAN: WiFi, VoIP, multimedia y seguridad, 2006, Editorial Limusa Noriega Editores, México
- MARTIN Juan Carlos, Instalaciones de Telecomunicaciones, técnicas básicas, EDITEX
- EC-Council; 2009; "Ethical Hacking and Countermeasures: Attack Phases (Ec-Council Press Series: Certified Ethical Hacker)"; Course Technology; 1 edition
- EC-Council; 2009; "Ethical Hacking and Countermeasures: Threats and Defense Mechanisms (Ec-Council Press Series: Certified Ethical Hacker)"; Course Technology; 1 edition
- EC-Council; 2009; Computer Forensics: Hard Disk and Operating Systems (Ec-Council Press Series: Computer Forensics)"; Course Technology; 1 edition (September 22, 2009)

Web:

- ISO/IEC 27001
- Fuente de información relacionada con: la Norma ISO27000 http://www.27005.net/
- Fuente de información relacionada con: la seguridad de la información: ISO 27001, Análisis del riesgo de la seguridad y soluciones de la política de la seguridad http://www.security.kirion.net/seguridad/
- Fuente de información relacionada con: la guía de seguridad de la información para Pymes http://www.vdigitalrm.com/archivos/guia_seguridad_pymes.pdf

BIBLIOGRAFÍA

Amparo. (s.f.). *Manual: Gestión de Incidentes de Seguridad Informatica.* Recuperado el Octubre de 2012, de http://www.proyectoamparo.net/files/manual_seguridad/manual_sp.pdf

Armando, C. (s.f.). *ACIS.* Recuperado el Octubre de 2012, de ACIS: http://www.acis.org.co/

Borrego, D. (27 de Marzo de 2009). *Herramientas para pymes.com.* Recuperado el Octubre de 2012, de Herramientas para pymes.com: http://www.herramientasparapymes.com/

Clavijo, C. A. (2006). *Politicas de Seguridad Informatica.*

Cruz, P. S. (Septiembre de 2012). *ISO 22301 - Continuidad del Negocio.* Recuperado el Enero de 2013, de http://www.interempresas.net/FeriaVirtual/Catalogos_y_documentos/87942/Continuidad_Negocio-ISO-22301.pdf

Cuate, M. U. (Octubre de 2011). *Sistema de Gestion de Continuidad del Negocio de Acuerdo con BS25999 e ISO 22301.* Recuperado el Noviembre de 2012, de http://sas-origin.onstreammedia.com/origin/isaca/LatinCACS/cacs-lat/forSystemUse/papers/133.pdf

Erb, M. (s.f.). *Gestión de Riesgo en la Seguridad Informática.* Recuperado el Enero de 2013, de Gestión de Riesgo en la Seguridad Informática: http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

Esplandiú, C. (s.f.). *British Standards Institution*. Recuperado el Octubre de 2012, de British Standards Institution: http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001/

Gómez Vieites, Á. (2007). *Enciclopedia de la Seguridad Informática.* GaliNova.

Gonzalo Álvarez Marañón. (2000). *Departamento de Tratamiento de la Información y Codificación*. Recuperado el Octubre de 2012, de Departamento de Tratamiento de la Información y Codificación: http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html

Internacional, E. (2005). *ISO/IEC 27001.*

ISO. (2012). *International Standard: Societal security : business continuity management systems : reqiurements. ISO 22301. gestion de la continuité des affaires. exigences.* ISO.

Kosutic, D. (s.f.). *IS&BCA.* Recuperado el Noviembre de 2012, de Information Security & Business Continuity Academy: http://www.iso27001standard.com

Latinoamérica, L. E. (s.f.). *Informe sobre malware en América Latina.*

libnova. (s.f.). Recuperado el Octubre de 2012, de libnova: http://www.libnova.es/seguridad.html

López Crespo Francisco, A. G. (2006). *Magerit I Metodo - Version 2.* Madrid.

López Crespo Francisco, A. G. (2006). *Magerit II Catalogo de Elementos - Version 2.* Madrid.

Mieres, J. (Enero de 2009). *Ataques informaticos.* Recuperado el Octubre de 2012, de Ataques informaticos: https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

Vignoni, I. J. (2002). *Control de Procesos.*