PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

E.S.E. HOSPITAL JOSE CAYETANO VÁSQUEZ

Trabajamos por un Puerto Boyacá Saludable!!!

2020

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

1. DOCUM ENTOS RE LACIONADOS

Normo grama MCC - FOR - 009 - V03
Manual mantenimiento sw y hw A2-S2-D-07
Política de seguridad y confidencialidad de la información A2-S2-D-15
Política de gerencia de la información A2-S2-D-16
Caracterización de proceso de gestión de la Tecnología A2-D-01

2. GLOSARIO

- A

Acción correctiva
(Inglés: Corrective action). Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.
Acción preventiva
(Inglés: Preventive action). Medida de tipo pro-activo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2005. En ISO 27001:2013, ya no se emplea; ha quedado englobada en Riesgos y Oportunidades.
Accreditation body
Véase: Entidad de acreditación.
Aceptación del riesgo
(Inglés: Risk acceptance). Decisión informada de asumir un riesgo concreto.
Activo
(Inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
Alcance
(Inglés: Scope). Ámbito de la organización que queda sometido al SGSI.
Amenaza
(Inglés: Threat). Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
Análisis de riesgos
(Inglés: Risk analysis). Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
Análisis de riesgos cualitativo
(Inglés: Qualitative risk analysis). Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.
Análisis de riesgos cuantitativo
(Inglés: Quantitative risk analysis). Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.
Asset
Véase: Activo.
Assets inventory
Véase: Inventario de activos.

Audit
Véase: Auditoría.
Auditor
(Inglés: Auditor). Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.
Auditor de primera parte
(Inglés: First party auditor). Auditor interno que audita la organización en nombre de ella misma.
Auditor de segunda parte
(Inglés: Second party auditor). Auditor que audita una organización en nombre de otra. Por ejemplo, cuando una empresa audita a su proveedor de outsourcing, o cuando una administración pública ordena una auditoriía de una empresa.
Auditor de tercera parte
(Inglés: Third party auditor). Auditor que audita una organización en nombre de una tercera parte independiente que emite un certificado de cumplimiento.
Auditor jefe
(Inglés: Lead auditor). Auditor responsable de asegurar la conducción y realización eficiente y efectiva de la auditoría, dentro del alcance y del plan de auditoría acordado.
Auditoría
(Inglés: Audit). Proceso sistemático, independiente y documentado para obtener evidencias de auditoriía y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.
Autenticación
(Inglés: Authentication). Provisión de una garantía de que una característica afirmada por una entidad es correcta.
Autenticidad
(Inglés: Authenticity). Propiedad de que una entidad es lo que afirma ser.
Authentication
Véase: Autenticación.
Availability
Véase: Disponibilidad.

- B

BS 7799
Norma británica de seguridad de la información, publicada por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera era un conjunto de buenas prácticas para la gestión de la seguridad de la información -no certificable- y la parte segunda especificaba el sistema de gestión de seguridad de la información -certificable-. La parte primera es el origen de ISO 17799 e ISO 27002 y la parte segunda de ISO 27001. Como tal estándar, ha sido derogado ya, por la aparición de éstos últimos.
BSI
British Standards Institution, la entidad de normalización del Reino Unido, responsable en su día de la publicación de la norma BS 7799, origen de ISO 27001. Su función como entidad de normalización es comparable a la de AENOR en España.
Business Continuity Plan
Véase: Plan de continuidad del negocio.

- C

Certification body Véase: Entidad de certificación.

CIA

CID

Véase: CID. Acrónimo inglés de confidentiality, integrity y availability, las dimensiones básicas de la seguridad de la información.

CISA

CISM

CISSP

(Inglés: CIA). Acrónimo español de confidencialidad, integridad y disponibilidad, las dimensiones básicas de la seguridad de la información.

Certified Information Systems Auditor. Es una acreditación ofrecida por ISACA.

Certified Information Security Manager. Es una acreditación ofrecida por ISACA.

Certified Information Systems Security Professional. Es una acreditación ofrecida por ISC2.

Checklist
Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.
Clear desk policy
Véase: Política de escritorio despejado.

CobiT

Control Objectives for Information and related Technology. Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Compromiso de la Dirección
(Inglés: Management commitment). Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. La versión de 2013 de ISO 27001 lo engloba bajo la cláusula de Liderazgo.
Confidencialidad
(Inglés: Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Confidentiality
Véase: Confidencialidad.
Contramedida
(Inglés: Countermeasure). Véase: Control.
Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
Control correctivo
(Inglés: Corrective control). Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.
Control detectivo
(Inglés: Detective control). Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.
Control disuasorio
(Inglés: Deterrent control). Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.
Control preventivo
(Inglés: Preventive control). Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.
Control selection
Véase: Selección de controles.
Corrección
(Inglés: Correction). Acción para eliminar una no conformidad detectada. Si lo que se elimina es la causa de la no conformidad, véase acción correctiva.
Correction
Véase: Corrección.
Corrective action
Véase: Acción correctiva.
Corrective control
Véase: Control correctivo.
Countermeasure
Contramedida. Véase: Control.

- D

Declaración de aplicabilidad

(Inglés: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.
Desastre

(Inglés: Disaster). Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.
Detective control
Véase: Control detectivo.
Deterrent control
Véase: Control disuasorio.
Directiva o directriz
(Inglés: Guideline). Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.
Disaster
Véase: Desastre.
Disponibilidad
(Inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

DRII DTI

- E

ENAC

Instituto Internacional de Recuperación de Desastres.

Secretaría de Industria y Comercio del Reino Unido. Edita muchas guías prácticas en el ámbito de la seguridad de la información.

Entidad Nacional de Acreditación. Es el organismo español de acreditación, auspiciado por la Administración, que acredita organismos que realizan actividades de evaluación de la conformidad, sea cual sea el sector en que desarrollen su actividad. Además de laboratorios, entidades de inspección, etc., también acredita a las entidades de certificación, que son las que a su vez certificarán a las empresas en las diversas normas.

Entidad de acreditación
(Inglés: Accreditation body). Un organismo oficial que acredita a las entidades certificadoras como aptas para certificar según diversas normas. Suele haber una por país. Son ejemplos de entidades de acreditación: ENAC (España), UKAS (Reino Unido), EMA (México), OAA (Argentina), etc. En nuestra sección Normalización y Acreditación figuran todas las de países de habla hispana.
Entidad de certificación
(Inglés: Certification body). Una empresa u organismo acreditado por una entidad de acreditación para auditar y certificar según diversas normas (ISO 27001, ISO 9001, ISO 14000, etc.) a empresas usuarias de sistemas de gestión.
Entidad de normalización
(Inglés: Standards body). Un organismo oficial que genera y publica normas. Suele haber una por país. Son ejemplos de entidades de normalización: AENOR (España), BSI (Reino Unido), DGN (México), IRAM (Argentina), etc. En nuestra sección Normalización y Acreditación figuran todas las de países de habla hispana.
Estimación de riesgos

(Inglés: Risk evaluation). Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.
Evaluación de riesgos
(Inglés: Risk assessment). Proceso global de identificación, análisis y estimación de riesgos.
Evidencia objetiva
(Inglés: Objective evidence). Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.

- F

Fase 1 de auditoría
(Inglés: Stage 1 Audit). Etapa de la auditoría de primera certificación en la que, fundamentalmente a través de la revisión de documentación, se analiza en SGSI en el contexto de la política de seguridad de la organización, sus objetivos, el alcance, la evaluación de riesgos, la declaración de aplicabilidad y los documentos principales, estableciendo un marco para planificar la fase 2.
Fase 2 de auditoría

(Inglés: Stage 2 Audit). Etapa de la auditoría de primera certificación en la que se comprueba que la organización se ajusta a sus propias políticas, objetivos y procedimientos, que el SGSI cumple con los requisitos de ISO 27001 y que está siendo eficaz.
First party auditor
Véase: Auditor de primera parte.

- G

Gestión de claves
(Inglés: Key management). Controles referidos a la gestión de claves criptográficas.
Gestión de incidentes de seguridad de la información
(Inglés: Information security incident management). Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
Gestión de riesgos
(Inglés: Risk management). Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
Guideline
Véase: Directiva.

- H

Humphreys, Ted
Experto en seguridad de la información y gestión del riesgo, considerado "padre" de las normas BS 7799 e ISO 17799 y, por tanto, de ISO 27001 e ISO 27002.

- I

Identificación de riesgos

(Inglés: Risk identification). Proceso de encontrar, reconocer y describir riesgos.

IEC

IIA
International Electrotechnical Commission. Organización internacional que publica estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas.

Instituto de Auditores Internos.

Impacto
(Inglés: Impact). El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-.
Impact
Véase: Impacto.
Incidente de seguridad de la información
(Inglés: Information security incident). Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Information processing facilities
Véase: Recursos de tratamiento de información.
Information security
Véase: Seguridad de la información.
Information security incident
Véase: Incidente de seguridad de la información.
Information security incident management
Véase: Gestión de incidentes de seguridad de la información.
Information Security Management System (ISMS)
Véase: Sistema de Gestión de Seguridad de la Información (SGSI).
Integridad
(Inglés: Integrity). Propiedad de la información relativa a su exactitud y completitud.
Integrity
Véase: Integridad.
Interested party
Véase: Parte interesada.
Inventario de activos
(Inglés: Assets inventory). Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

IRCA

International Register of Certified Auditors. Acredita a los auditores de diversas normas, entre ellas ISO 27001.

ISACA

ISC2

ISMS ISO

Information Systems Audit and Control Association. Publica CobiT y gestiona diversas acreditaciones personales en el ámbito de la auditoría de sistemas y la seguridad de la información.

Information Systems Security Certification Consortium, Inc. Organización sin ánimo de lucro que gestiona diversas acreditaciones personales en el ámbito de la seguridad de la información.

Information Security Management System. Véase: SGSI.

Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).

ISO 17799
Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. Dio lugar a ISO 27002, por cambio de nomenclatura, el 1 de Julio de 2007. Ya no está en vigor.
ISO 19011
“Guidelines for auditing management systems”. Norma con directrices para la auditoría de sistemas de gestión. Guía de utilidad para el desarrollo, ejecución y mejora del programa de auditoría interna de un SGSI.
ISO/IEC 27001
Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.
ISO/IEC 27002
Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.
ISO 9001
Norma que establece los requisitos para un sistema de gestión de la calidad.

ISSA ITIL

ITSEC

Information Systems Security Association.

IT Infrastructure Library. Un marco de gestión de los servicios de tecnologías de la información.

- J

JTC1

- K

Criterios de evaluación de la seguridad de la tecnología de información. Se trata de criterios unificados adoptados por Francia, Alemania, Holanda y el Reino Unido. También cuentan con el respaldo de la Comisión Europea (véase también TCSEC, el equivalente de EEUU).

Joint Technical Committee. Comité técnico conjunto de ISO e IEC específico para las tecnologías de la información.

Key management
Véase: Gestión de claves.

- L

Lead auditor
Véase: Auditor jefe.

- M

Management commitment
Véase: Compromiso de la Dirección.

- N

NBS NIST

Oficina Nacional de Normas de los EE.UU.

(ex NBS) Instituto Nacional de Normas y Tecnología, con sede en Washington, D.C.

No conformidad
(Inglés: Nonconformity). Incumplimiento de un requisito.
Nonconformity
Véase: No conformidad.
No repudio
Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.

Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

- O

Objective evidence
Véase: Evidencia objetiva.
Objetivo
(Inglés: Objetive). Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

- P

Parte interesada
(Inglés: Interested party / Stakeholder). Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
PDCA
Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.
Plan de continuidad del negocio
(Inglés: Bussines Continuity Plan). Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.
Plan de tratamiento de riesgos
(Inglés: Risk treatment plan). Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
Política de escritorio despejado
(Inglés: Clear desk policy). La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.
Preventive action
Véase: Acción preventiva.
Preventive control

Véase: Control preventivo.
Proceso
(Inglés: Process). Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.
Process
Véase: Proceso.
Propietario del riesgo
(Inglés: Risk owner). Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

- Q

Qualitative risk analysis
Véase: Análisis de riesgos cualitativo.
Quantitative risk analysis
Véase: Análisis de riesgos cuantitativo.

- R

Recursos de tratamiento de información
(Inglés: Information processing facilities). Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.
Residual risk
Véase: Riesgo residual.
Riesgo

(Inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
Riesgo residual
(Inglés: Residual risk). El riesgo que permanece tras el tratamiento del riesgo.
Risk
Véase: Riesgo.
Risk acceptance
Véase: Aceptación del riesgo.
Risk analysis
Véase: Análisis de riesgos.
Risk assessment
Véase: Evaluación de riesgos.

Risk evaluation
Véase: Estimación de riesgos.
Risk identification
Véase: Identificación de riesgos.
Risk management
Véase: Gestión de riesgos.
Risk owner
Véase: Propietario del riesgo.
Risk treatment
Véase: Tratamiento de riesgos.
Risk treatment plan
Véase: Plan de tratamiento de riesgos.
• S
Safeguard
Salvaguarda. Véase: Control.
Salvaguarda
(Inglés: Safeguard). Véase: Control.
Sarbanes-Oxley
Ley de Reforma de la Contabilidad de Compañías Públicas y Protección de los Inversores aplicada en EEUU desde 2002. Crea un consejo de supervisión independiente para supervisar a los auditores de compañías públicas y le permite a este consejo establecer normas de contabilidad así como investigar y disciplinar a los contables. También obliga a los responsables de las empresas a garantizar la seguridad de la información financiera.

SC27

Scope

Subcomité 27 del JTC1 (Joint Technical Committee) de ISO e IEC. Se encarga del desarrollo de los estándares relacionados con técnicas de seguridad de la información..

Véase: Alcance.

Second party auditor
Véase: Auditor de segunda parte.
Segregación de tareas
(Inglés: Segregation of duties). Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Segregation of duties
Véase: Segregación de tareas.
Seguridad de la información
(Inglés: Information security). Preservación de la confidencialidad, integridad y disponibilidad de la información.
Selección de controles
(Inglés: Control selection). Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.
SGSI
(Inglés: ISMS). Véase: Sistema de Gestión de la Seguridad de la Información.
Sistema de Gestión de la Seguridad de la Información
(Inglés: Information Security Management System). Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

SoA

SSCP

Acrónimo inglés de Statement of Applicability. Véase: Declaración de aplicabilidad.

Systems Security Certified Practitioner. Una acreditación personal de ISC2.

Stage 1 Audit
Véase: Fase 1 de auditoría.
Stage 2 Audit
Véase: Fase 2 de auditoría.
Stakeholder
Véase: Parte interesada.
Standards body
Véase: Entidad de normalización.
Statement of Applicability (SoA)
Véase: Declaración de aplicabilidad.
• T
Third party auditor
Véase: Auditor de tercera parte.
Threat

Véase: Amenaza.

Tratamiento de riesgos
(Inglés: Risk treatment). Proceso de modificar el riesgo, mediante la implementación de controles.
Trazabilidad
(Inglés: Accountability). Según [CESID: 1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

- U

UNE 71502
Norma española de ámbito local como versión adaptada de BS7799-2. Ya no está en vigor.

- V

Vulnerabilidad
(Inglés: Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas.
Vulnerability
Véase: Vulnerabilidad.

- W

WG1, WG2, WG3, WG4, WG5
WorkGroup 1, 2, 3, 4, 5. Grupos de trabajo del subcomité SC27 de JTC1 (Joint Technical Committee) de ISO e IEC. Estos grupos de trabajo se encargan del desarrollo de los estándares relacionados con técnicas de seguridad de la información.

3. OBJETIVO DEL PLAN.

Especificar los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI), con las mejores prácticas descritas en ISO/IEC 27002, que permita minimizar los riesgos de pérdida de activos de la información en la E.S.E HOSPITAL JOSE CAYETANO VASQUEZ, teniendo en cuenta el auto diagnóstico de la dimensión de Gobierno digital de acuerdo a la metodología del Modelo Integrado de Planeación y Gestión mipg.

4. ALCANCE.

El plan aplica a todas las áreas de la E.S.E HOSPITAL JOSE CAYETANO VASQUEZ y a los designados de las mismas, tanto para la obligatoriedad de la información a divulgar, como la forma correcta de publicación y las acciones de mejora a que haya lugar.

5. INTRODUCCION

El plan de seguridad de la información son aquellos procedimientos y herramientas aplicadas, que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Basados en la norma ISO 27799:2008 que define las directrices que pueden apoyar la interpretación y la aplicación al sector sanitario de las ya conocidas ISO 27001 y 27002, puesto que especifica un conjunto detallado de controles para la gestión de la seguridad de la información específicas para el ámbito sanitario y nos proporciona una serie de claras directrices de seguridad sobre las mejores prácticas a seguir en los temas relacionados con la salud.

Mediante la aplicación de esta norma internacional, las organizaciones sanitarias y entidades afines serán capaces de garantizar un nivel mínimo de seguridad necesaria para que pueda mantenerse en ellas de manera coherente la confidencialidad, integridad y disponibilidad de los datos personales referentes a la salud.

ISO 27799:2008 es aplicable a la información sanitaria en todos sus aspectos y en cualquiera de sus formas (palabras y cifras o coeficientes, grabaciones sonoras, dibujos, vídeo e imágenes médicas o radiografías), sobre cualquier medio de almacenamiento (escrito o impreso en papel y electrónico) y a través de cualquier medio de transmisión (valijas o mensajería, faxes, redes informáticas o correo electrónico).

Esta norma hace referencia a la seguridad de la información, pero siempre mediante una gestión orientada a las necesidades del sector sanitario a través del control de sus específicos entornos operativos. Si bien la protección y la seguridad de la información personal son importante para todas las personas, empresas, instituciones y gobiernos, existen requisitos especiales en este sector que deben satisfacerse para garantizar la confidencialidad, la integridad y la disponibilidad de la información médico-asistencial.

Proteger la confidencialidad se hace mandatorio, puesto que los datos personales referentes a la salud deben de ser tratados - en la mayoría de los países - con el nivel más alto de protección.
Por otra parte, es indispensable mantener la integridad de la información médico-sanitaria, para garantizar la seguridad de los pacientes, además de garantizar que este tipo de información sea auditable fielmente durante todo su ciclo de vida.

Por último, la disponibilidad de información referente a la salud también es fundamental para la eficacia de la prestación de servicios médicos. Los sistemas informáticos sanitarios deben de cumplir con la única premisa de permanecer en funcionamiento tanto en situaciones de desastre natural, como en fallos del sistema o durante eventuales ataques de denegación de servicio.
Por tanto, la protección de la confidencialidad, la integridad y la disponibilidad de la información de índole médico, requiere de un conocimiento y una experiencia específicos en la materia que han sido reunidos en esta norma, que no pretende suplantar a la ISO 27001 o 27002 sino complementarlas puesto que estas pueden ser aplicadas a organizaciones de todo tipo, mientras que la ISO 27799 ha sido creada contemplando las mejores prácticas llevadas a cabo en diversos centros de atención primaria, en clínicas, por equipos de atención domiciliaria, en hospitales, en consultas de especialistas, etc. con la única finalidad de incorporar una aproximación a la realidad del sector sanitario para controlar su seguridad de manera eficaz.

6. RESPONSABILIDAD DEL MANUAL

Los cambios, modificaciones o actualizaciones del presente manual, está a cargo del Líder del proceso de sistemas de información.

7. NORMATIVA

La normativa en que se basa en el plan de seguridad y privacidad de la información, contempla las directrices y recomendaciones de:

- ISO 27000 contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.

- ISO 27001: Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

- ISO 27002: Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005.

- ISO 27003: Consiste en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

- ISO 27004: Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.

- ISO 27005: Publicada el 4 de Junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la

seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 y ISO/IEC TR 13335-4:2000.

- ISO 27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

- ISO 27007: Se encuentra en fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de auditoría de un SGSI.

- ISO 27011: Consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

- ISO 27031: Se encuentra en fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

- ISO 27032: Consiste en una guía relativa a la Ciberseguridad.

- ISO 27033: Se encuentra en fase de desarrollo; su fecha prevista de publicación es entre 2010 y 2011. Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante Gateway, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y re numeración de ISO 18028.

- ISO 27034: Consiste en una guía de seguridad en aplicaciones.

- ISO 27799: Publicada el 12 de Junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma. ISO 27799:2008 especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias

que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud. ISO 27799:2008 se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas, toma la información (palabras y números, grabaciones sonoras, dibujos, vídeos e imágenes médicas), sea cual fuere el medio utilizado para almacenar (de impresión o de escritura en papel o electrónicos de almacenamiento) y sea cual fuere el medio utilizado para transmitirlo (a mano, por fax, por redes informáticas o por correo), ya que la información siempre debe estar adecuadamente protegida.

- ISO 27799:2008 La norma no es nueva. Desde 2003 ya viene trabajando el grupo de trabajo TC215 WG4 y desde finales de 2006 la norma ya era pública en la comunidad científica. La norma ISO 27799:2008 específica para el ámbito sanitario define las directrices que pueden apoyar la interpretación y la aplicación al sector de las ya mencionadas ISO 27001 y 27002. Específica un conjunto detallado de controles para la gestión de la seguridad de la información específica para el ámbito específico y nos proporciona una serie de claras directrices de seguridad sobre las mejores prácticas a seguir en los temas relacionados con la salud. Esta norma es aplicable a la información sanitaria en todos sus aspectos y en cualquiera de sus formas (palabras, números, grabaciones sonoras, dibujos, vídeo e imágenes médicas o radiografías), sobre cualquier medio de almacenamiento (escrito o impreso en papel y electrónico) y a través de cualquier medio de transmisión (valijas o mensajería, faxes, redes informáticas o correo electrónico).

8. SEGURIDAD FISICA Y DEL ENTORNO

El uso adecuado de los recursos tecnológicos asignados por HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. a sus funcionarios y/o terceros se reglamenta bajo los siguientes lineamientos:

a) La instalación de cualquier tipo de software o hardware en los equipos de cómputo de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. es responsabilidad del proceso de Gestión de la tecnología, encabezada por el profesional de gestión de la tecnología, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. a través del proceso de Gestión de la tecnología de la información.

b) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios pueden ser realizados únicamente por los miembros del proceso de Gestión de la tecnología de la información.

c) proceso de Gestión de la tecnología de la información debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

d) Únicamente los funcionarios y terceros autorizados por el proceso de Gestión de la

tecnología de la información, previa solicitud escrita por parte de la dependencia que lo requiera, pueden conectarse a la red inalámbrica de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E.

e) La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. Deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por el proceso de Gestión de la tecnología de la información.

f) Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E.; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidas por el proceso de Gestión de la tecnología de la información.

g) La sincronización de dispositivos móviles, tales como PDAs, smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Organización, debe estar autorizado de forma explícita por la dependencia respectiva, en conjunto con el proceso de Gestión de la tecnología de la información y podrá llevarse a cabo sólo en dispositivos provistos por la organización, para tal fin.

8.1 Escritorio y pantalla limpia

[ISO/IEC 27001:2005 A.11.2.4]

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida manera inmediata.

Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco
(5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

8.2 Acuerdos de confidencialidad
[ISO/IEC 27001:2005 A.6.1.5]

Todos los funcionarios de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la Institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de la Institución a personas externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

8.3 Riesgos relacionados con terceros
[ISO/IEC 27001:2005 A.6.2.2]

HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. Identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

Los controles que se establezcan como necesarios a partir del análisis de riesgos, deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

OBJETIVO DEL PROCESO: Garantizar la disponibilidad de la Tecnología necesaria para el funcionamiento de los procesos institucionales con eficiencia, eficacia, efectividad y seguridad para los usuarios, colaboradores y medio ambiente.

8.4 Uso adecuado de los activos
[ISO/IEC 27001:2005 A.7.1.3]
[Acuerdos 047 y 056 de 2000 Archivo General de la Nación]

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios y contratistas determinadas por los Jefes de Área o Dependencia.

Para la consulta de documentos cargados en el Tutorial de Calidad, se establecerán privilegios de acceso a los funcionarios y/o contratistas. Dichos privilegios serán establecidos por el Jefe de la oficina de Calidad.

Todos los funcionarios y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un “acuerdo de confidencialidad de la información”, donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la

información; y que cualquier violación a lo establecido en este parágrafo será considerado como un "incidente de seguridad".

9. ACCESO A INTERNET

El internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

9.1 No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

- El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN Messenger, Yahoo, Skype, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E.

- El intercambio no autorizado de información de propiedad de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E., de sus clientes y/o de sus funcionarios, con terceros.

- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

- Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

- Los funcionarios y terceros, al igual que los empleados o subcontratistas de estos, no pueden asumir en nombre de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E., posiciones personales en encuestas de opinión, foros u otros medios similares.

- El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E.

10. CORREO ELECTRÓNICO

Los funcionarios y terceros autorizados a quienes HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

- La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E., así mismo podrá ser utilizada para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad.

- Los mensajes y la información contenida en los buzones de correo son propiedad de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

- El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deberán ser definidos e implementados por la Dirección de Tecnología.

No es permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

- Utilizar la dirección de correo electrónico de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. como punto de contacto en comunidades interactivas de contacto social, tales como facebook y/o MySpace, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.

- El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

- El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal.

- Toda información de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. generada con los diferentes programas computacionales (Ej. Office, Project, Access, Wordpad, etc.), que requiera ser enviada fuera de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E., y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por la Dirección de Tecnología. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el

receptor requiera hacer modificaciones a dicha información.

 Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

11. PROTECCION DE LA INFORMACION

11.1 Control de acceso físico
[ISO/IEC 27001:2005 A.9.1]

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tal que puedan ser auditadas (como videos de grabación), así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales. De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

11.2 Protección y ubicación de los equipos
[ISO/IEC 27001:2005 A.9.2]

Los equipos que hacen parte de la infraestructura tecnológica de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. Tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Los funcionarios y terceros, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica de

HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.
HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. mediante mecanismos adecuados monitoreará las condiciones ambientales de las zonas donde se encuentren los equipos (Centros de Cómputo).

11.3 Análisis de Requerimientos de seguridad

[ISO/IEC 27001:2005 A.12.1.1]

Los requerimientos de seguridad de la información identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor deben ser establecidos en los acuerdos contractuales que se realicen entre HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información. Es responsabilidad del Gerente garantizar la definición y establecer la clausulas correspondientes en los documentos contractuales.

11.4 Protección contra software malicioso
[ISO/IEC 27001:2005 A.10.4]

HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red institucional, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso.

Será responsabilidad del proceso de Gestión de la tecnología de la información, autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

Así mismo, HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. define los siguientes lineamientos: No está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por la ESE HOSPITAL JOSE CAYETANO VASQUEZ.
- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.
- El uso de código móvil. Éste sólo podrá ser utilizado si opera de acuerdo con las políticas y normas de seguridad definidas y debidamente autorizado por la Dirección de Tecnología.

12. CONTROL DE ACCESO

12.1 Control de acceso lógico
[ISO/IEC 27001:2005 A.11.1]

El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias de la Institución, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.

Los responsables de la administración de la infraestructura tecnológica de la institución, asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos formales de autorización los cuales deben ser revisados de manera periódica por la Oficina de Control Interno de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E.

La autorización para el acceso a los sistemas de información debe ser definida y aprobada por la dependencia propietaria de la información, o quien ésta defina, y se debe otorgar de acuerdo con el nivel de clasificación de la

Información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los funcionarios y terceros e implementada por la Dirección de Tecnología.

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E., sea por Internet, acceso telefónico o por otro medio, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

13. RESPONSABILIDADES Y ROLES

13.1 Gestión de contraseñas de usuario
[ISO/IEC 27001:2005 A.11.2.3]

Todos los recursos de información críticos de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada funcionario requiera para el desarrollo de sus funciones, definidos y aprobados por las áreas de negocio y administrados por la Dirección de Tecnología.

Todo funcionario o tercero que requiera tener acceso a los sistemas de información de la ESE HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso de un usuario (ID) y contraseña (password). El funcionario debe ser responsable por el buen uso de las credenciales de acceso asignadas.

14. TRANSMISION DE INFORMACIÓN Y COMUNICACIÓN

14.1 Segregación de redes
[ISO/IEC 27001:2005 A.11.4.5]

La plataforma tecnológica de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes de terceros y del servicio de acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. La Dirección de Tecnología es el área encargada de establecer el perímetro de

seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. establece mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de la Organización.

Es responsabilidad de los administradores de recursos tecnológicos garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

15. CUSTODIA DE LA INFORMACION

15.1 Intercambio de información

[ISO/IEC 27001:2005 A.10.8] [Resolución 1995 de 1999 – Normas para el Manejo de la Historia Clínica]

HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. Dispondrá de cláusulas contractuales de conformidad de confidencialidad con el personal que disponga de permisos de acceso a información clasificada o reservada como es el caso de la Historia clínica, [Resolución 1995 de 1999 – Normas para el Manejo de la Historia Clínica.

Todo funcionario de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos.

16. **PLAN DE CONTINGENCIA**

16.1 Gestión de medios removibles

[ISO/IEC 27001:2005 A.10.7]

El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas) sobre la infraestructura para el procesamiento de la información de la ESE HOSPITAL JOSE CAYETANO VASQUEZ funciones lo requiera.

El proceso de Gestión de la tecnología de la información es responsable de implementar

los controles necesarios para asegurar que en los sistemas de información de HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. sólo los funcionarios autorizados pueden hacer uso de los medios de almacenamiento removibles.

Así mismo, el funcionario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de la ESE HOSPITAL JOSE CAYETANO VASQUEZ que éste contiene.

16.2 Falla general eléctrica y/o del sistema de la HISTORIA CLINICA DIGITAL.

Una vez sea reportada la falla a cualquier miembro del proceso de Gestión de la tecnología, el profesional de Gestión de la tecnología deberá hacer revisión en la ESE Hospital José Cayetano Vásquez donde presenta el inconveniente.

Si la falla es por problemas eléctricos, con ayuda del profesional de infraestructura se determinará el tiempo que durara dar una solución; Si el problema es por fallas en la red de datos o del sistema mismo, será responsabilidad por parte del profesional de Gestión de la tecnología de terminar el tiempo que durara la falla.

En el caso que el tiempo estimado en dar solución al problema sea mayor de 60 minutos, el profesional de Gestión de la tecnología tendrá que buscar un medio eficiente y eficaz, para dar a conocer al director del HJCV, la activación del plan del plan de contingencia.

Es responsabilidad del director del HJCV, que haya disponibilidad física de los formatos necesarios para diligenciamiento de los borradores de historias clínicas y coordinar con los auxiliares de enfermería, la entrega de estos formatos a los profesionales que lo necesiten, para qué puedan seguir atendiendo a los pacientes mientras se da solución definitiva al inconveniente.

El director del HJCV deberá determinar cuántas historias clínicas se dejaron de ingresar por profesional al sistema y garantizar un horario en la semana para que ellos puedan realizar el cargue respectivo de la información a la historia clínica sistematizada.

El profesional de la salud debe utilizar este horario designado por el director del HJCV, para realizar el cargue de la historia clínica completa, de forma cuidadosa y responsable, que garantice que la información escrita en los borradores coincida en su totalidad a la ingresada al sistema.

Una vez el profesional haya ingresado la historia clínica sistematizada, deberá hacer entrega de los borradores al director del HJCV, para que el corrobore que la totalidad de los borradores y su información haya sido ingresada al sistema por parte del profesional, con el fin de proceder a la destrucción de los borradores de la historia clínica.

Los documentos que contengan, firmas, huellas u cualquier otro método que de constancia de la aprobación de un procedimiento por parte del usuario, como consentimientos informados, deberán ser entregados al área de archivo, en el cual la persona responsable de archivo, dispondrá de un día para escanear estos documentos de forma organizada y

almacenarlos en una carpeta, que serán cargadas de forma automática a la historia clínica sistematizada.

16.3 Copias de respaldo
[ISO/IEC 27001:2005 A.10.5]

HOSPITAL JOSE CAYETANO VASQUEZ E.S.E. debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por Gerencia, Sub gerencias y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la Institución como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

Del proceso de Gestión de la tecnología de la información establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma.

Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

17. FUENTES

- ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems - Requirements
- ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management
- ISO/IEC 27006:2007 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management (anterior ISO/IEC 17799:2005)
- ISO 9001:2000, Quality management systems — Requirements
- ISO/IEC 13335-1:2004, Information technology — Security techniques —

Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management

- ISO/IEC TR 13335-3:1998, Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security
- ISO/IEC TR 13335-4:2000, Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards
- ISO 14001:2004, Environmental management systems — Requirements with guidance for use
- ISO/IEC TR 18044:2004, Information technology — Security techniques — Information security incident management
- ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing.