PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION EN LA

E.S.E HOSPITAL DE NAZARETH

OFICINA DE SISTEMAS DE INFORMACION
2021 - 2024

INTRODUCCIÓN

La E.S.E. Hospital de Nazareth Siempre ha visto la información como un activo importante para la atención de los servicios de salud y el desarrollo de sus procesos institucionales, por lo tanto, se preocupa por definir lineamientos que permitan mitigar los posibles riesgos para la Información.

El plan de seguridad y privacidad de la información es un documento que contiene los lineamientos que apoyan la gestión y administración de los planes y procedimientos de seguridad de la información dando claridad sobre las prácticas de seguridad aplicadas a la institución.

1. ALCANCE

El plan contempla la estructura y los lineamientos principales para la seguridad de la información en la E.S.E. Hospital de Nazareth Los lineamientos definidos en este documento deben ser conocidos y cumplidos por empleados, contratistas y todos los terceros que tengan acceso, almacenen, procesen o trasmitan información de la institución o sus pacientes.

La Política de Seguridad Informática del E.S.E HOSPITAL DE NAZARETH aplicara a todos los activos de información de la institución.

La E.S.E HOSPITAL DE NAZARETH define como Activos de Información:

- Elementos de Hardware y de Software de procesamiento.
- Dispositivos de Almacenamiento y comunicaciones.
- Bases de Datos y Procesos.
- Procedimientos y Recursos Humanos asociados con el manejo de los datos.
- La Información Misional, Operativa y Administrativa del E.S.E HOSPITAL DE NAZARETH.
- Elementos de hardware y de software de la ESE HOSPITAL DE NAZARETH.

De la misma forma estas políticas están orientadas a garantizar el uso apropiado de los dispositivos tecnológicos (computadores de escritorio, portátiles, equipos de audiovisuales etc.) y de servicios como el Internet y Correo Electrónico, brindando a los funcionarios pautas para la utilización apropiada de dichos recursos, permitiendo así minimizar los riesgos de una eventual pérdida.

Estas Políticas aplican a todos los funcionarios, contratistas, o terceras personas que accedan a los activos de información del Hospital, con las respectivas autorizaciones, los cuales están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de seguridad de información que los trabajadores de la institución.

2. OBJETIVO GENERAL

Establecer los lineamientos principales de ley y gestión de la seguridad de la información para la E.S.E. Hospital de Nazareth.

3. DEFINICIONES

3.1. Activos de información: Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada departamento.
Este tipo de activo representa los datos de la organización, información que tiene valor para los procesos Clínicos y/o Administrativos, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil.

3.2. Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada, modificada o adulterada a individuos, entidades o procesos no autorizados.

3.3. Control: Es toda actividad o procesos encaminados a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

3.4. Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

3.5. Evento de seguridad de la información: Se considera un Evento de Seguridad de la Información a cualquier situación identificada que indique una posible brecha en la Política de Información o falla en los controles y/o protecciones establecidas.

3.6. Incidente de seguridad de la información: Un incidente de seguridad de la información se define como un acceso, uso, divulgación, modificación o destrucción no autorizada de la información de la E.S.E. Hospital de Nazareth y de sus usuarios; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Información.

3.7. Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

3.8. Propietario/responsable de activo de información: Empleado de la Empresa que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

3.9. Servicio: Es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

3.10. Usuario: Es el nombre (o alias) que se le asigna a cada persona para ser identificado por el servidor, de esta manera el proveedor de Internet o de correo electrónico lo identifica, es única en cada servidor, y cada usuario tiene asignado una contraseña para poder acceder a su cuenta.

3.11. Factores de riesgos. - Manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgo o tienden a aumentar la exposición, pueden ser interna o externa a la entidad.

3.12. Impacto. - Es la medición y valoración del daño que podría producir a la empresa un incidente de seguridad. La valoración global se obtendrá sumando el coste de reposición de los daños tangibles y la estimación, siempre subjetiva, de los daños intangibles.

3.13. Riesgo. - Proximidad o posibilidad de un daño, peligro, etc. Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro.

3.14. Seguridad. - Cualidad o estado de seguro. Garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo. Se dice también de todos aquellos objetos, dispositivos, medidas, etc., que contribuyen a hacer más seguro el funcionamiento o el uso de una cosa: cierre de seguridad, cinturón de seguridad.

3.15. Seguridad física. - Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención ante amenazas a los recursos e información confidencial que puedan interrumpir procesamiento de información.

3.16. Seguridad lógica. - Consiste en la aplicación de barreras y procedimientos para mantener la seguridad en el uso de software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

3.17. Seguridad de las redes. - Es la capacidad de las redes para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas, que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes ofrecen o hacen accesibles y que son tan costosos como los ataques intencionados.

3.18. Seguridad en los recursos humanos. - Consiste en los controles que se deben tener con respecto a la selección, contratación, capacitación y despido del empleado.

3.19. Seguridad Informática. - Son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados.

3.20. Vulnerabilidad. - Cualquier debilidad en los Sistemas de Información que pueda permitir a las amenazas causarles daños y producir pérdidas.

4. NORMATIVIDAD RELACIONADA

Para la construcción de este plan se tiene como base, la norma ISO – IEC 27001:2013 Sistema de Gestión de la Seguridad de la Información, el modelo de gestión de la seguridad de la información y la política de información de la E.S.E. Hospital de Nazareth.

5. COMPROMISO DE LA DIRECCIÓN

La Junta Directiva y la Gerencia de la E.S.E. Hospital de Nazareth muestra su compromiso y apoyo en el diseño, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información a través de la asignación de recursos, la definición de la política de información, los lineamientos de seguridad

6. PROPÓSITO

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera establecida por la institución y que el acceso a la información allí contenida, así como su modificación sólo sea permitido a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Para que un sistema se pueda definir como seguro debe tener estas cuatro características

- **Integridad:** La información sólo puede ser modificada por quien está autorizado.
- **Confidencialidad:** La información sólo debe ser legible para los autorizados.
- **Disponibilidad:** Debe estar disponible cuando se necesita.
- **Irrefutabilidad:** (No-Rechazo o No Repudio) Que no se pueda negar la autoría.

7. POLITICA DE SEGURIDAD DE LA INFORMACION

En la ESE HOSPITAL DE NAZARETH estamos comprometidos en satisfacer las necesidades de comunicación e información a los grupos de interés internos y externos, cumpliendo con las características de confiabilidad, oportunidad y confidencialidad, a través de mecanismos eficaces para la divulgación y circulación.

La E.S.E HOSPITAL DE NAZARETH si lo considera necesario, ajustará sus Políticas de Seguridad Informática a través de un acto administrativo.
Las políticas de seguridad informática de la E.S.E HOSPITAL DE NAZARETH, identifican responsabilidades y establecen los objetivos para una protección de los activos de información de la organización.

8. CUMPLIMIENTO

El cumplimiento de las Políticas de Seguridad es obligatorio y extensible a todos los funcionarios, contratistas, o terceras personas que accedan a los activos de Información del Hospital. El incumplimiento de las políticas por negligencia o intencionalidad, hará que la E.S.E HOSPITAL DE NAZARETH, tome las medidas correspondientes, tales como acciones disciplinarias, suspensión del contrato de prestación de servicios, acciones legales, reclamo de compensación por daños, entre otras acciones de tipo administrativo.

9. ACCESO A LOS RECURSOS DE INFORMACIÓN:

Todos los funcionarios, contratistas, o terceras personas que accedan a los activos de información del Hospital deben ser autorizados previamente sin discriminación alguna por parte del Coordinador de Sistemas y tienen los siguientes deberes

- Se debe custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función, conserve bajo su cuidado o a la cual tenga acceso, impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidas de la información institucional.
- Se debe proteger los softwares, los aplicativos, los equipos de comunicación y procesamiento de datos, que le han sido asignados para su utilización de acuerdo al uso de las buenas prácticas, de manera racional y de conformidad con los fines a que han sido destinados.
- El acceso a los sistemas y recursos de información solamente se debe permitir si existe autorización. Esta autorización es asignada por el Profesional de Sistemas, previa aprobación del gerente.
- El acceso a los recursos de información de la organización presupone la aceptación de este documento de políticas de seguridad, así como las respectivas sanciones por su incumplimiento, lo cual se confirma a través de la firma de un acuerdo de responsabilidad que hará parte del contrato prestación de servicios o acto de posesión.
- Los funcionarios del Hospital, deben garantizar que el acceso a la información y la utilización de la misma sea exclusivamente para actividades relacionadas con las funciones propias de la organización y

que esta sea utilizada de acuerdo a los criterios de confidencialidad definidos por la E.S.E HOSPITAL DE NAZARETH.

10. PROTECCIÓN DE LA INFORMACIÓN

Los activos de información serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida de los activos de la información del E.S.E HOSPITAL DE NAZARETH. La protección debe acentuar la confidencialidad, integridad y disponibilidad de los activos de información.

Todos los funcionarios, contratistas, o terceras personas que accedan a los activos de información del Hospital deben:

- Definir y ejecutar procedimientos de seguridad para la entrega de información, apoyándose de algunos lineamientos muy claros donde se determine qué información se considera confidencial, restringida o pública.
- La copia de seguridad de información exógena al Sistema de Información Institucional, es responsabilidad de todos los funcionarios, contratistas, o terceras personas que accedan a estos activos informáticos.

- Esta información deberá ser entregada o cargada al servidor por medio de la red o disco externo cada 15 días.

11. PROTECCIÓN DE LOS RECURSOS TECNOLÓGICOS

La E.S.E HOSPITAL DE NAZARETH asegurará la contratación requerida para mantener actualizadas las licencias de Antivirus, Firewall, el mantenimiento de las redes y equipos, e infra estructuras de las mismas, las cuales permitirán proteger los recursos informáticos contra ataques de virus, ingresos maliciosos y filtrados de contenido de correos, archivos, USB, CD, etc.

Los recursos tecnológicos serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida del negocio. Dichos recursos deben ser utilizados exclusivamente para desarrollar las actividades laborales y así mismo, su utilización se hará en forma adecuada, con el máximo de eficiencia y con ejemplar racionalidad.

La infraestructura de los Servidores y equipos de telecomunicaciones del Hospital, debe estar ubicada en un área protegida o cerrada (Centro de Cableado o Centro de Cómputo) en la cual sólo se permitirá el ingreso de personal autorizado, es decir, a quienes deban cumplir alguna función específica relacionada con dichos equipos. Debe establecerse un registro de acceso al centro de cableado donde se indiquen los horarios y funciones realizadas (bitácora).

12. AUTORIZACIÓN DE USUARIOS

Todos los usuarios deben ser identificados independientemente con permisos de acceso específicamente e individualmente autorizados. Los métodos de acceso de usuarios deben exigir un proceso robusto de autenticación, autorización apropiada y auditoría confiable. Para cumplir con esta política el Profesional de Sistemas del Hospital, debe definir las consideraciones a tener en cuenta para la autorización y permisos de los usuarios.

En el caso de los usuarios de e-salud, la solicitud la debe realizar el respectivo líder del módulo o Coordinador de área pertinente con las siguientes características.

- Nombre de usuario.
- Número de identificación.
- Permisos correspondientes.

13. RESPONSABILIDAD

Los usuarios y custodios de los activos de información del E.S.E HOSPITAL DE NAZARETH, son responsables por el uso apropiado, protección y privacidad de estos activos. Los sistemas generarán y mantendrán unas apropiadas reglas de auditoría para identificar usuarios, y documentar los eventos relacionados con la seguridad y Disponibilidad.

Los activos de información deben estar disponibles para soportar los objetivos de la E.S.E HOSPITAL DE NAZARETH. Deben tomarse medidas adecuadas para asegurar el tiempo de recuperación de toda la información y acceso por individuos autorizados.

El área de sistemas del Hospital debe definir el plan de recuperación en conjunto con los usuarios involucrados en el proceso, para garantizar la continuidad del negocio.

14. INTEGRIDAD

Los activos de información deben estar adecuadamente protegidos para asegurar su integridad y precisión. Las medidas de validación definidas permitirán detectar la modificación inapropiada, eliminación o adulteración de los activos de información.

15. LINEAMIENTO DE SEGURIDAD.

15.1 Gestión de activos

- Las diferentes áreas con el fin de garantizar la administración y control

sobre los activos de la entidad, deben mantener un inventario actualizado de los activos que se encuentran dentro del alcance del modelo de gestión de seguridad de la información y que están cargados a cada proceso, el cual debe estar alineado con el inventario general de activos de información.

- En el inventario se identificará el propietario del activo, quien debe asegurar que la información y los activos asociados con su proceso están clasificados de manera apropiada, así como de establecer controles necesarios para el acceso a éstos de acuerdo con los procedimientos definidos.

16. USO ACEPTABLE DE LOS ACTIVOS

- La información, archivos físicos, los sistemas, los servicios y los equipos (estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad del Hospital de Nazareth, son activos de la Institución y se proporcionan a los funcionarios, contratistas y terceros autorizados, para cumplir con los propósitos del negocio.

- El Hospital de Nazareth podrá monitorear, supervisar y utilizar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en esta manual y en cualquier proceso legal que se requiera.

- 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, contratistas y terceros determinadas por los Líderes de área.

- La consulta de expedientes o documentos que reposan en las diferentes oficinas y/o áreas del Hospital de Nazareth se permitirá en días y horas laborales, con la presencia del funcionario o servidor responsable de aquellos.

- El Líder o Director del área, serán quienes determinen el carácter de reserva o restricción de los documentos físicos. 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 lineamientos definidos en la Política de Información del Hospital de

Nazareth y los lineamientos del presente documento. En caso de violación de la información será considerado como un incidente de seguridad y se procederá de acuerdo a lo definido al tratamiento de este tipo de incidentes.

16.1 Acceso a Internet:

- **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 que tengan como objetivo crear comunidades para intercambiar información o bien para fines diferentes a las actividades propias del Hospital.
  - El Intercambio no autorizado de información de propiedad del Hospital, de sus clientes, usuarios 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.
  - La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el Líder respectivo y la Líder de los estándares de Gerencia de la Información, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

- La E.S.E. Hospital de Nazareth puede realizar monitoreo de tiempos de navegación y páginas visitadas por parte de los funcionarios, contratistas y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

- 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, contratistas y terceros, al igual que los empleados o subcontratistas de estos, no pueden asumir en nombre del Hospital, posiciones personales en encuestas de opinión, foros u otros medios de comunicación externos 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 del Hospital de Nazareth.

16.2 Correo electrónico:

- El correo electrónico corporativo es una herramienta de comunicación o intercambio de información oficial entre personal o instituciones, no es una herramienta de difusión indiscriminada de información.

- La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro del Hospital.

- Los mensajes y la información contenida en los buzones de correo son propiedad del Hospital de Nazareth y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

- El tamaño de los buzones de correo es determinado por el área de Sistemas de la entidad de acuerdo con las necesidades de cada usuario y previa autorización del Jefe y/o Líder del área correspondiente.

- El tamaño de envío y recepción de mensajes, sus contenidos y demás características propias de estos deberán ser definidos e implementados por el área de Sistemas del Hospital de Nazareth.

- El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que el Hospital de Nazareth proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal dentro de la institución.

- El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación del área de Comunicaciones y la autorización del área de Sistemas del Hospital. Además, para terceros se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a nombre del área

respectiva y/o servicio habilitado para tal fin y no a través de cuenta de correo electrónico asignadas a un usuario particular.

- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por el Hospital de Nazareth y deben conservar en todos los casos el mensaje legar corporativo de confidencialidad.

- Los archivos que se adjuntan en los mensajes de correo en lo posible deben comprimirse para evitar la saturación en las diferentes cuentas de correos.

- El usuario que tiene asignada una cuenta de correo electrónico es el único y directo responsable de todas las acciones y mensajes que se lleven a cabo en su nombre, por lo tanto, el Hospital no se hace responsable por lo que diga o haga. Esta información se incluirá en todos los mensajes que se envíen.

- Las únicas áreas de la institución autorizadas para enviar mensajes a través de la lista de correo denominada personal en la cual se incluyen todas las direcciones de correo del Hospital son: La Gerencia, Comunicaciones, Sistemas y Recursos Humanos.

- El correo electrónico corporativo es la única vía de remisión o envío de documentos de carácter administrativo interno en el hospital.

No está 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 del Hospital de Nazareth, como punto de contacto en comunidades interactivas de contacto social, tales como Facebook, Instagram, 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.

16.3 Recursos tecnológicos:

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo del Hospital de Nazareth es responsabilidad del área de Sistemas, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por el Hospital a través de esta área.

- 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 son realizados únicamente por el área de Sistemas.

- El área de Sistemas del hospital definirá y actualizará, de manera periódica, la lista de software y aplicaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones instaladas y administradas por el Hospital.

- Los funcionarios serán conectados a la red de la ESE HOSPITAL DE NAZARETH con previa solicitud escrita y autorizada por el Líder del área. Los terceros y/o contratistas se conectarán a la red de la ESE HOSPITAL DE NAZARETH, bajo los lineamientos del área de Sistemas, asegurando la legalidad del equipo a través de certificados emitidos por la empresa contratista, de acuerdo a lo definido por el área de sistemas.

- Los usuarios que requieren acceder a la infraestructura tecnológica del HOSPITAL DE NAZARETH desde redes externas, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por el área de Sistemas. Además, deberán informar previamente a la misma área para autorizar el acceso y brindar los permisos respectivos para la protección de la información, de acuerdo a lo definido por el área de sistemas.

- Ningún funcionario contratista o tercero podrá copiar para uso personal archivos o programas de propiedad del Hospital.

17. Acuerdos sobre confidencialidad

- Todos los funcionarios, colaboradores y/o terceros que presten sus servicios al Hospital de Nazareth, deberán 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 los 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 del Hospital de Nazareth, a personas o entidades 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.
- 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.

18. Clasificación de la información

- El Hospital de Nazareth con el fin de resguardar la información que pueda ser divulgada de forma no autorizada o manipulada erróneamente por parte de sus funcionarios, contratistas, proveedores o clientes, ha establecido niveles para la clasificación de la información, incluyendo la información que puede encontrarse en medio electrónico, impreso, verbal o que sea transmitida por cualquier medio.

- Toda la información del Hospital de Nazareth debe ser identificada, clasificada y documentada de acuerdo con los criterios de clasificación establecidos por el Comité Institucional de Gestión y Desempeño.
- Los niveles de clasificación de la información definidos en el Hospital de Nazareth son:
  - EXTERNA
  - CATEGORÍA PÚBLICA
  - PÚBLICA USO INTERNO
  - PÚBLICA CLASIFICADA
  - PÚBLICA RESERVADA

19. Seguridad de los recursos humanos

- Todos los funcionarios del Hospital de Nazareth, contratistas y terceros que tengan la posibilidad de acceder a la información de la organización y a la infraestructura para su procesamiento, son responsables de conocer y cumplir con las políticas y procedimientos establecidos en el Modelo de Gestión de Seguridad de la Información del Hospital de Nazareth. De igual forma, son responsables de reportar

por medio de los canales apropiados, el incumplimiento de las políticas y procedimientos establecidos.

- Todos los funcionarios del Hospital de Nazareth deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de la organización.

- Todos los funcionarios del Hospital de Nazareth, deben hacer buen uso de la escarapela que los acredita como sus servidores, este documento debe ser devuelto al Hospital de Nazareth en el momento de su desvinculación.

19.1 Educación, formación y concientización sobre la Seguridad de la Información

- El Hospital de Nazareth debe asegurar que todos los funcionarios que tengan definidas responsabilidades en la Seguridad de la Información son competentes para desempeñar sus funciones y que cuentan con los programas de capacitación y entrenamiento requeridos para ello.
- De igual forma, todos los funcionarios y, cuando sea relevante, los terceros tendrán un proceso formal de concientización, mediante el cual se capacitará sobre las políticas de seguridad de la Institución y los riesgos conocidos a los que se puede ver expuesta, en caso que estas no se cumplan.
- Los programas de concientización, educación y entrenamiento se encuentran diseñados de manera apropiada y relevante para los roles, responsabilidades y habilidades de las personas que deben asistir a ellos.

19.2 Proceso disciplinario

- En el caso de identificarse un incidente de seguridad, éste será registrado en la herramienta de gestión designada, y se hará la investigación respectiva para determinar las causas y responsables posteriormente, el Hospital de Nazareth, tomará las acciones pertinentes para el funcionario y/o tercero vinculado con el incidente, mediante un proceso disciplinario formal de acuerdo con la naturaleza, gravedad y/o el impacto que haya podido generar a la organización dicho incidente de acuerdo a los procedimientos del proceso Gestión Disciplinaria.

19.3 Devolución de Activos.

- Todo funcionario al momento de su retiro o cambio de funciones en la institución debe hacer entrega a su jefe inmediato del equipo que se le había asignado, adjuntado un inventario con toda la información contenida en él. .

20. Seguridad física y del entorno

- El Hospital de Nazareth será el responsable de definir el perímetro de la seguridad física de acuerdo a la clasificación de los activos de la información, controlando el acceso a la información a través de controles (Ejemplo: acceso a áreas restringidas con tarjeta, registro de entrada de equipos, autenticación), los cuales disminuyen la posibilidad de riesgo de divulgación o pérdida de información.

20.1 Controles de Acceso Físico

- 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 área de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, 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.

- Las áreas de carga, descarga, entrega de mercancías y demás puntos de acceso a las instalaciones del Hospital de Nazareth, deben ser controladas y en lo posible separadas de las áreas seguras para evitar el acceso no autorizado a estas últimas.

- Los funcionarios, contratistas y terceros del Hospital de Nazareth, así como los visitantes, deben portar su identificación y/o escarapela de manera visible durante el tiempo que permanezca dentro de las instalaciones de la organización.
- En caso de retiro o desvinculación laboral del funcionario, contratistas

y/o tercero, éste debe hacer devolución de la respectiva escarapela asignada en desarrollo de sus funciones, previa liquidación de sus prestaciones sociales y demás obligaciones.

20.2 Protección y ubicación de los equipos

- Los equipos que hacen parte de la Infraestructura tecnológica del Hospital de Nazareth, 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 o brinden servicios de soporte a la información crítica de las áreas, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.

- Los funcionarios y terceros, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica del Hospital de Nazareth no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.

- Cualquier traslado de equipos de cómputo se realizará con la coordinación del área de Sistemas previa verificación de las condiciones técnicas y de seguridad.

- Toda persona que note algún problema de funcionamiento o ataque de virus en una estación de trabajo debe reportarlo de inmediato al personal de soporte técnico del Departamento de Sistemas mediante el uso de los canales de comunicación definidos para ello.

- El Hospital de Nazareth mediante mecanismos adecuados monitoreará las condiciones ambientales de las zonas donde se encuentren los equipos.

- El Hospital de Nazareth debe proveer suministros y equipamiento de soporte como electricidad, aire acondicionado, planta eléctrica y un sistema de alimentación no interrumpida (UPS) que asegure el tiempo necesario para apagar adecuadamente los servidores donde se alojan los sistemas de información ante una falla en el suministro de cualquiera de estos elementos, evitando así la pérdida o corrupción de información. Estos suministros deben ser monitoreados, revisados y medidos permanentemente para asegurar su funcionamiento y condiciones normales de operación y evitar futuros daños.

- De igual manera, el Hospital de Nazareth, debe establecer un programa de planeación y ejecución de mantenimientos preventivos anuales (como mínimo), a la infraestructura tecnológica.

- Ningún empelado, contratista o tercero podrá desarmar o destapar equipos sin la autorización previa del Departamento de Sistemas.

20.3 Seguridad de los equipos y medios de información fuera de las instalaciones

- Independientemente del propietario, todos los funcionarios son responsables de velar por la seguridad de los equipos del Hospital de Nazareth que se encuentren fuera de las instalaciones de la organización.

- Bajo ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.

- Los equipos de infraestructura del Hospital de Nazareth, deben ser transportados con las medidas de seguridad apropiadas, que garanticen la integridad física de los dispositivos.

- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

- Los equipos del Hospital de Nazareth, deberán contar con un seguro que los proteja de robo.

- En caso de pérdida o robo de un equipo del Hospital de Nazareth, se deberá informar inmediatamente al Líder del Proceso para que se inicie el trámite interno y se deberá poner la denuncia ante la autoridad competente.

- El retiro de equipos de cómputo, periféricos, dispositivos de almacenamientos, software e información considerada crítica propiedad de Hospital de Nazareth, fuera de las instalaciones de la organización debe seguir los procedimientos establecidos por el área de Sistemas del Hospital de Nazareth.

20.4 Eliminación o reutilización segura de equipos y medios

- El Hospital de Nazareth debe identificar los riesgos potenciales que puede generar destruir, reparar o eliminar equipos y medios de almacenamiento. Para ello, debe definir e implementar los mecanismos y controles adecuados para que la información sensible contenida en ellos sea eliminada de manera segura.

- Cuando un equipo sea reasignado o dado de baja, se deberá realizar el proceso de acuerdo al procedimiento establecido para tal fin.