



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 1 de 95</p> |

Sistema de Gestión de Seguridad Informática y Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información *Versión 03*

GOBIERNO DIGITAL INSTITUTO DEPARTAMENTAL DE SALUD DE NORTE DE SANTANDER

CARLOS ARTURO MARTINEZ GARCIA
Director

LAURY LISBETH PAEZ PARADA
Coordinador Jurídica y Control Disciplinario

JOSE TRINIDAD URIBE
Coordinador Salud Pública

JOSE ANTONIO GUTIERREZ
Coordinador Atención en Salud

CARMEN ELENA SEPULVEDA AYALA
Coordinadora Recursos Financieros



HENRY GIOVANNI MANTILLA BLANCO
Coordinador Recursos Humanos

MARÍA VICTORIA GIRALDO RUIZ
Coordinadora de Planeación

LUIS ARMANDO ROJAS CAICEDO
Líder de Sistemas de Información

Enero de 2021





| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 2 de 95</p> |

CONTENIDO



| | |
|--|----|
| INTRODUCCIÓN..... | 8 |
| 1. SITUACIÓN ACTUAL..... | 10 |
| 1.1 Objetivos estratégicos..... | 10 |
| 1.2 La Planeación Estratégica. | 12 |
| 1.2.1 Misión..... | 12 |
| 1.2.2 Visión..... | 12 |
| 1.2.3 Objetivo General..... | 12 |
| 1.2.4 Funciones Institucionales:..... | 12 |
| 1.2.5 Organigrama | 15 |
| 1.3 El Plan Integral de Desarrollo..... | 16 |
| 2. ESTRATEGIAS QUE INTEGRAN LA SEGURIDAD DE LA INFORMACIÓN A LA ESTRATEGIA ORGANIZACIONAL..... | 17 |
| 3. POLÍTICAS DE SEGURIDAD..... | 21 |
| 3.1. Política general de seguridad..... | 22 |
| 3.1.1 Introducción..... | 22 |
| 3.1.2 Objetivo General..... | 23 |
| 3.1.3 Objetivos Específicos..... | 23 |
| 3.1.4 Alcance..... | 24 |
| 3.1.5 Política..... | 24 |
| 3.2 Política particular para el uso adecuado de estaciones de trabajo | 31 |
| 3.2.1 Objetivo..... | 31 |
| 3.2.2 Alcance..... | 32 |
| 3.2.3 Responsabilidades | 32 |
| 3.2.4 Violaciones y Sanciones | 32 |
| 3.2.5 Política..... | 33 |
| 3.3 Política particular para el control de acceso..... | 39 |



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 3 de 95</p> |

| | | |
|--------|--|-----------|
| 3.3.1 | Objetivo..... | 39 |
| 3.3.2 | Alcance..... | 39 |
| 3.3.3 | Responsabilidades | 39 |
| 3.3.4 | Violaciones y sanciones | 40 |
| 3.3.5 | Política..... | 40 |
| 3.4 | Política particular para el uso de Dispositivos de Almacenamiento de Información..... | 43 |
| 3.4.1 | Objetivo..... | 43 |
| 3.4.2 | Alcance..... | 44 |
| 3.4.3 | Responsabilidades | 44 |
| 3.4.4 | Violaciones y sanciones | 44 |
| 3.4.5 | Política..... | 45 |
| 4. | INFORME DE ANÁLISIS DE LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN..... | 48 |
| 4.1 | Caracterización de los Activos de Información | 49 |
| 4.2 | Valoración de Activos..... | 50 |
| 4.3 | Caracterización de las amenazas | 53 |
| 4.4 | Valoración de las amenazas..... | 54 |
| 4.5 | Estimación del estado del riesgo | 56 |
| 4.6 | Análisis de Resultado de la Valoración y Definición de los Riesgos..... | 61 |
| 5. | SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN | 63 |
| 5.1 | Controles del Sistema de gestión de Seguridad de la Información..... | 63 |
| 5.2 | Indicadores Propuestos para el Sistema de Gestión de Seguridad de la Información | 67 |
| 5.3. | Valoración de acuerdo a los controles..... | 68 |
| 5.3.1. | Resultados de la Valoración..... | 70 |
| 6. | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION | 74 |
| 6.1. | Valoración De Incidentes – Modelo Ponemon | 76 |
| 7. | ANALISIS DE AMENAZAS Y RIESGOS EMERGENTES EN SEGURIDAD DE LA INFORMACION | 81 |
| 7.1. | Análisis de incertidumbres..... | 83 |





| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 4 de 95</p> |

CONCLUSIONES 84

BIBLIOGRAFÍA..... 85

ANEXO 89





| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 5 de 95</p> |

LISTAS DE ILUSTRACIONES

| | |
|--|----|
| Ilustración 1 Grupos y dependencias IDS | 11 |
| Ilustración 2. Organigrama del IDS | 15 |
| Ilustración 3 Mapa de Macroprocesos y Procesos del IDS | 21 |
| Ilustración 4. Valoración del riesgo..... | 57 |
| Ilustración 5. Rango de Riesgo | 57 |
| Ilustración 6. Valoración de Datos e información de acuerdo a las amenazas originadas por la criminalidad | 58 |
| Ilustración 7. Valoración de Datos e información de acuerdo a las amenazas originadas Por sucesos de origen físico | 58 |
| Ilustración 8. Valoración de Datos e información de acuerdo a las amenazas originadas Por sucesos derivados de la impericia, negligencia de usuarios/as Y decisiones institucionales | 59 |
| Ilustración 9. Valoración de Sistemas e Infraestructura de acuerdo a las amenazas Originadas por la criminalidad..... | 59 |
| Ilustración 10. Valoración de Sistemas e Infraestructura de acuerdo a las amenazas Originadas por sucesos de origen físico | 60 |
| Ilustración 11. Valoración de Sistemas e Infraestructura de acuerdo a amenazas Originadas por sucesos derivados de la impericia, negligencia de usuarios/as y Decisiones institucionales | 60 |
| Ilustración 12 Valoración del Riesgo | 70 |
| Ilustración 13 Valoración del Riesgo (Continuación) | 71 |
| Ilustración 14 Valoración del Riesgo (Continuación) | 72 |
| Ilustración 15 Valoración del Riesgo (Continuación) | 73 |
| Ilustración 16 Plan de Tratamiento de los riesgos | 74 |
| Ilustración 17 Plan de Tratamiento de los riesgos (Continuación) | 75 |
| Ilustración 18 Aspectos a tener en cuenta modelo Ponemon Institute..... | 76 |
| Ilustración 19 Valores de los costos internos..... | 78 |





| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 6 de 95</p> |

LISTA DE TABLAS

| | | |
|-----------|---|----|
| Tabla 1 | Generalidades de la empresa | 10 |
| Tabla 2 | Servicios que ofrece el IDS | 13 |
| Tabla 3. | Servicios que ofrece el IDS (Continuación)..... | 14 |
| Tabla 4 | Servicios que ofrece el IDS (continuación) | 15 |
| Tabla 5. | Matriz DOFA Seguridad de la Información | 18 |
| Tabla 6. | Matriz DOFA Seguridad de la Información (continuación) | 19 |
| Tabla 7. | Tipo de impacto o magnitud del daño | 51 |
| Tabla 8 | Tabla de impacto o magnitud | 52 |
| Tabla 9 | Activos de Información Sistemas e Información | 52 |
| Tabla 10. | Origen de la Amenaza..... | 53 |
| Tabla 11. | Tabla de Probabilidad..... | 55 |
| Tabla 12 | Amenazas por actos originados por la criminalidad común y motivación política | 55 |
| Tabla 13 | Amenazas por sucesos de origen físico | 56 |
| Tabla 14 | Amenaza por sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales..... | 56 |
| Tabla 15. | Opciones de manejo de los riesgos..... | 57 |
| Tabla 16 | Resultado del análisis de riesgo con evaluación Medio | 61 |
| Tabla 17 | Resultado de análisis de riesgo con evaluación Alto | 62 |
| Tabla 18 | Definición de Controles para el SGSI | 65 |
| Tabla 19. | Definición de Controles para el SGSI (Continuación)..... | 66 |
| Tabla 20 | Relación de Indicadores por Controles..... | 68 |
| Tabla 21 | Parámetros de valoración para los Controles | 69 |
| Tabla 22 | Rango de calificación de los controles..... | 69 |
| Tabla 23 | Valoración de costos | 77 |
| Tabla 24 | Diez (10) Incidentes de seguridad según Kaspersky | 77 |
| Tabla 25 | Valores de los costos externos..... | 79 |
| Tabla 26 | Resumen de costos basado en Modelo Ponemon Institute | 80 |





| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 7 de 95</p> |

LISTA DE ANEXOS

Anexo 1. Definición de indicadores propuestos.....90



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 8 de 95</p> |


INTRODUCCIÓN

Hoy en día, existen amenazas fuera y dentro de la organización por ende nos vemos en la necesidad de implementar un SGSI para la protección de datos dentro de las organizaciones públicas y privadas, que permita garantizar la confidencialidad, integridad y disponibilidad para la toma de decisiones aportando al mejoramiento continuo y logro de los objetivos estratégicos y para ello a la vez se debe implementar sistemas de gestión de riesgo en la seguridad informática.

Al hablar de una organización pública se deben aceptar cambios enfocados a mantener seguridad en los datos a través de políticas, normas, con personal idóneo y capacitado que ayuden de forma estratégica a buscar medidas preventivas que permitan proteger la información de manera responsable, eficiente y eficaz.

“la información debe ser vista como otro recurso de toda organización igualmente importante que traspasa las fronteras de todo proceso administrativo”. (Rivas Fernández, 2003), es necesario salvaguardar y proteger la información que produce, procesa y almacena el Instituto Departamental de Salud, como activo fundamental para el diseño de estrategias que permitan el fortalecimiento y mejoramiento continuo del proceso de salud pública en el departamento y contribuya al desarrollo de sus funciones como ente de dirección Departamental.




| | | |
|---|--|---|
| <p>NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 9 de 95</p> |

La identificación de los activos información es primordial e importante dentro del Instituto departamental de salud lo cual permite clasificar e edificar las amenazas y riesgos con probabilidad de daños a medida de escala o niveles en pérdida de información por causa de código malicioso que pueden estar surgiendo dentro de la organización. Por ello se definen los riesgos reales para proteger la información de los riesgos conocidos y se proponen controles a implementar.

Durante el desarrollo del presente trabajo se analiza la situación actual del Instituto Departamental de Salud de Norte de Santander con el objeto de conocer los objetivos estratégicos, la planeación estratégica y plan de desarrollo con el fin de proponer estrategias de mejoramiento a través de la implementación de Políticas de Seguridad de Información, e igualmente, se implementa una metodología que permite realizar un análisis de la gestión del riesgo con el fin de analizar y determinar los riesgos en los activos de la información de manera clasificada. Además, se aplica el modelo de Ponemon Institute para incidentes definidos por Kaspersky. Finalmente, se define la matriz ventana de AREM que es una herramienta estratégica y táctica para visualizar la incertidumbre para el análisis de amenazas y riesgos emergentes.



| | | |
|-------------------------------------|-------------------------------------|--|
| NORTE DE SANTANDER | DIRECCIONAMIENTO ESTRATEGICO |  Gobernación de Norte de Santander Instituto Departamental de Salud |
| Código: F-DE-PE05-04 Versión: 05 | COMUNICACION INTERNA | Página 10 de 95 |

1. SITUACIÓN ACTUAL

El Instituto Departamental de Salud de Norte de Santander (IDS) es una entidad del orden departamental con autonomía administrativa y financiera.

Tabla 1 Generalidades de la empresa



| | |
|-----------------------------|---|
| Entidad | Instituto Departamental de Salud de Norte de Santander – IDS |
| Tipo de Organización | Publica del orden departamental |
| Ubicación | Avenida 0 #9-60, edificio Rosetal, Ciudad San José de Cúcuta. |
| Sector: | Salud |
| Creada: | En 1975 |

Fuente. Elaboración propia.

1.1 Objetivos estratégicos.

- Realizar seguimiento a la ejecución del Plan de Desarrollo Departamental de Salud 2020- 2023
- Realizar seguimiento a la Implementación del Plan Decenal de Salud Publica 2012- 2021
- Cumplir lo reglamentado en la Resolución 2514 de 2012 para la vigencia 2020 – 2021) - Plan Bienal de Inversiones en Salud 2020 – 2021.
- Dar cumplimiento en los Estándares de Habilitación
- Fortalecer el Sistema de Gestión de Proyectos de Inversión del Instituto Departamental de salud.
- Coordinar la Implementación y desarrollo del Plan de Acción de Gobierno Digital
- Dar seguimiento a la implementación de software adquirido.

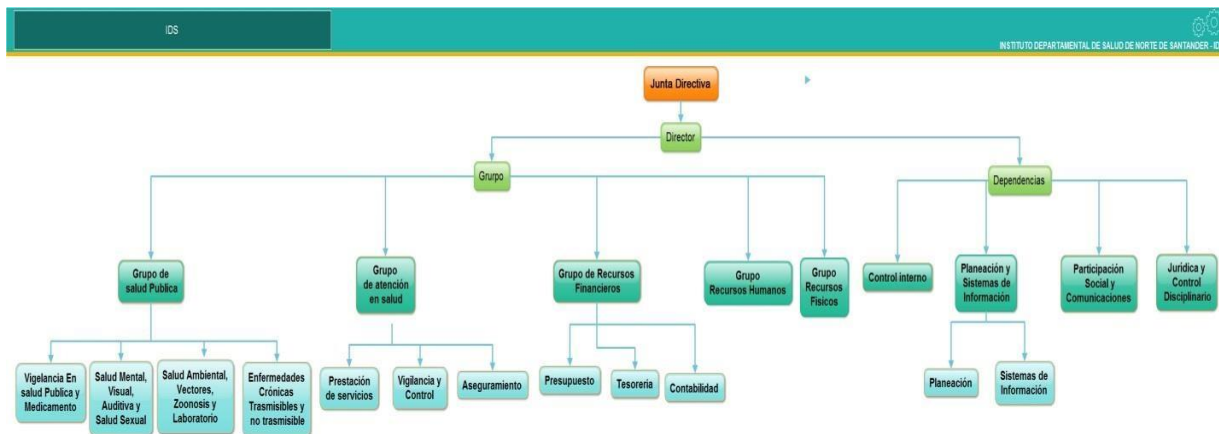


| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 11 de 95</p> |

- Mantener actualizado el sitio web institucional.
- Mantener en correcto funcionamiento los recursos de hardware y software de la entidad.
- Fortalecer los sistemas de Información de la Entidad.



El IDS cuenta con cinco grupos funcionales, los cuales son: Grupo de salud pública, grupo de atención en salud, grupo financiero, grupo de recursos físicos y grupo de recursos humanos, también cuenta con 4 dependencias y/u oficinas las cuales son: Planeación y Sistemas de Información, Control Interno, Participación Social y Jurídica y Control disciplinario; cada una de ellas tiene una funcionalidad para realizar en pro de la entidad y así lograr los objetivos misionales.

Ilustración 1 Grupos y dependencias IDS



Fuente. Elaboración propia



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 12 de 95</p> |

1.2 La Planeación Estratégica.

1.2.1 Misión

El Instituto Departamental de Salud de Norte de Santander en virtud de la ley 100 de 1993 y la ley 715 de 2001 contribuirá a crear condiciones de acceso de la población a los servicios de salud, como un servicio público a cargo del estado y a mejorar y mantener la calidad de vida de los habitantes del Departamento, mediante la dirección, coordinación, asesoría, vigilancia y control de los actores del Sistema de Seguridad Social en Salud, de tal forma que los servicios se presten con criterios de equidad, integridad, participación, eficiencia, oportunidad y calidad. (IDS, 2020)

1.2.2 Visión

“Ser el ente de Dirección Departamental de Salud participe del desarrollo social, líder del aseguramiento de toda la población al Sistema General de Seguridad Social en Salud, con especial énfasis en la población pobre y vulnerable”. (IDS, 2020)

1.2.3 Objetivo General

“El Instituto Departamental de Salud de Norte de Santander, tendrá como objetivo primordial dirigir, coordinar y vigilar el sector salud y el Sistema General de Seguridad Social en Salud en el territorio del Departamento Norte de Santander”. (IDS, 2020)

1.2.4 Funciones Institucionales:

- Dirección del sector Salud en el ámbito Departamental
- Prestación de Servicios de Salud.
- Salud Pública.
- Aseguramiento de la población al SGSSS.





| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 13 de 95</p> |

Tabla 2 Servicios que ofrece el IDS

| Grupos y Dependencias del IDS | Funcionalidad |
|---|---|
| <ul style="list-style-type: none"> • Dirección | <p>Formular políticas institucionales y adopción de planes, programas y proyectos tendientes a promover el desarrollo integral del sector salud del Departamento.</p> |
| <ul style="list-style-type: none"> • Jurídica y control disciplinario | <p>Coordinar la gestión jurídica del Instituto Departamental de Salud que propenda por el cumplimiento de la normatividad legal vigente en toda la gestión de la entidad y realizando asesoría y asistencia jurídica directamente al Director y funcionarios de las dependencias del Instituto.</p> |
| <ul style="list-style-type: none"> • Salud pública | <p>Diseñar estrategias que permitan el fortalecimiento y mejoramiento continuo del proceso de salud pública en Norte de Santander, para el logro del desarrollo operativo y funcional del Plan de Salud Pública Departamental.</p> |
| <p>Recursos financieros</p> | <p>Coordinar, ejecutar, asesorar y controlar las actividades de orden financiero tendientes a promover el desarrollo integral de los recursos financieros, presupuestales y contables de la Entidad.</p> |
| <p>Atención en salud</p> | <p>Desarrollar los procesos de aseguramiento al interior del IDS que permitan que la operación del régimen subsidiado garantice el acceso al aseguramiento de forma oportuna y ofrezca garantía en la integralidad y calidad de la prestación de los servicios de salud a la población más pobre y vulnerable de cada uno de los municipios del departamento. Garantizar el cumplimiento de las normas del sistema obligatorio de garantía de calidad en salud en el Departamento Norte de Santander.</p> |
| <p>Recursos humanos</p> | <p>Establecer políticas y estrategias orientadas a la gestión y administración del talento humano, asegurando la competencia y procurando el bienestar y la satisfacción de los usuarios internos y externos en pro de mejorar las condiciones de los funcionarios.</p> |
| <p>Planeación y sistemas de información</p> | <p>Organizar el desarrollo y ejecución de los propósitos y objetivos institucionales mediante la formulación de planes que orienten a las áreas estratégicas de la institución de la realización de las metas misionales en cumplimiento de los lineamientos nacionales en salud.</p> |

Fuente. Elaboración propia basada en información del IDS, 2021





| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 14 de 95</p> |

Tabla 3. Servicios que ofrece el IDS (Continuación)

| Grupos y Dependencias del IDS | Funcionalidad |
|--------------------------------------|--|
| Control interno | Fortalecimiento del desarrollo de la política de administración de riesgos a través del acompañamiento en su identificación y el seguimiento de los mismos, Asesorando y aplicando métodos de control, evaluación y seguimiento al Sistema de Control Interno, de manera independiente, posibilitando la búsqueda de la igualdad, eficiencia, eficacia, celeridad, calidad y economía de los diferentes procesos encaminados al cumplimiento de objetivos y metas misionales de manera transparente. |
| Vigilancia y control | Vigilar y controlar el cumplimiento de la normatividad legal vigente que regula el Sistema general de Seguridad Social en Salud, mediante el seguimiento continuo a los actores e involucrados en el sistema, con el fin de garantizar la Salud Pública del departamento Norte de Santander. Garantizar en forma integral el cumplimiento del sistema obligatorio de garantía de calidad en salud en el Departamento Norte de Santander. |
| Control de vectores | Contribuir al mejoramiento de la salud de la población de departamento mediante el desarrollo de estrategias y acciones de promoción, prevención, y vigilancia y control de las Enfermedades de Transmisión por Vectores. Con talento humano competente, comprometido y capacitado para brindar una atención oportuna, cálida y eficaz. |
| Laboratorio | Encargado del desarrollo de acciones técnico administrativas realizadas en atención a las personas y el medio ambiente con propósitos de vigilancia de eventos de interés en salud pública, gestión de la calidad e investigación, vigilancia y control sanitario |
| Salud ambiental | Contribuir al mejoramiento de la salud de la población del departamento mediante el desarrollo de estrategias de inspección, vigilancia y control, a los factores de riesgo del ambiente. |

Fuente. Elaboración propia basada en información del IDS, 2021





| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 15 de 95</p> |

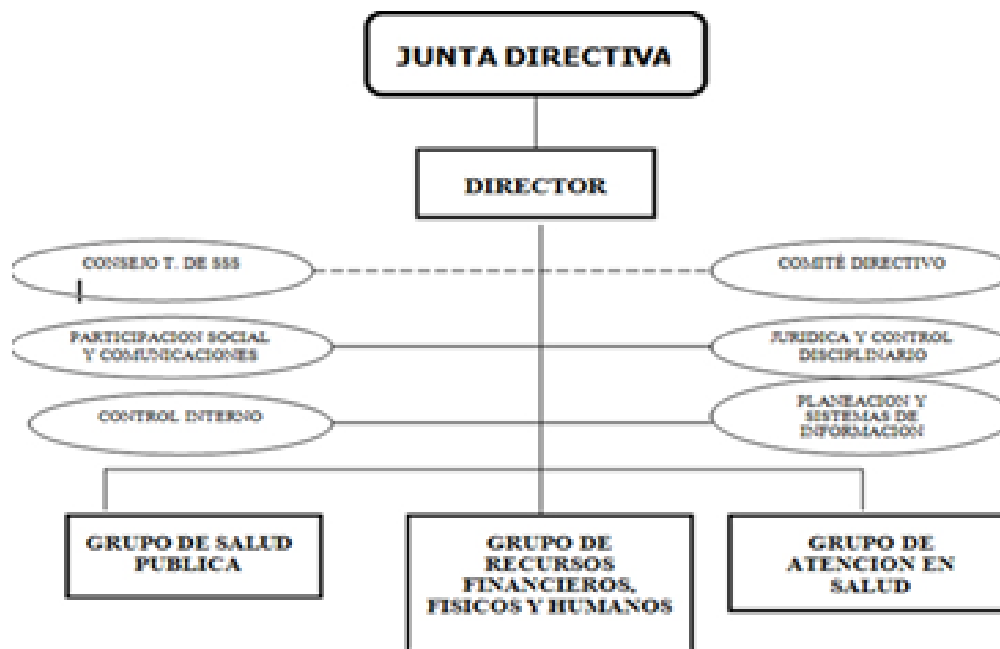
Tabla 4 Servicios que ofrece el IDS (continuación)

| Grupos y Dependencias del IDS | Funcionalidad |
|---|--|
| <p>Participación social y comunicaciones</p> | <p>Programar las acciones que se desarrollan desde el área de participación social y comunicaciones, servicio de atención a la comunidad, para la vigencia del año en curso, dando cumplimiento a lo establecido en el decreto 1757/94 y a la Resolución 1536 de 2015.</p> |
| <p>Prestación de servicios</p> | <p>Garantizar en forma integral y con calidad la prestación de servicios de salud a la población no afiliada a cargo del Departamento Norte de Santander.</p> |

Fuente. Elaboración propia basada en información del IDS, 2021



1.2.5 Organigrama

Ilustración 2. Organigrama del IDS



Fuente. Tomada de la página web del IDS, 2021





| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 16 de 95</p> |

1.3 El Plan Integral de Desarrollo.

Es la sostenibilidad de una serie de políticas que trabajan conjuntamente para fomentar el desarrollo de la entidad constituida como servicio nacional de Salud de Norte de Santander cuyo objetivo es trabajar para apoyar, facilitar, controlar, dirigir y promover el desarrollo integral del sector salud del Departamento.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 17 de 95</p> |

2. ESTRATEGIAS QUE INTEGRAN LA SEGURIDAD DE LA INFORMACIÓN A LA ESTRATEGIA ORGANIZACIONAL

Cano (2000) define que las Políticas de Seguridad de la Información “deben ir acompañadas de una visión de negocio que promueva actividades que involucren a las personas en su diario hacer, donde se identifiquen las necesidades y acciones que materializan las políticas”, por tal razón, las estrategias de seguridad de la información no son responsabilidad únicamente del personas de apoyo de las áreas de tecnología, sino que es responsabilidad de todos los funcionarios y contratistas que de una u otra forma estén vinculados con la producción, reproducción y custodia de la información existente, acorde con los objetivos estratégicos de la Entidad y contando con el apoyo y respaldo fundamental de la dirección.





| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 18 de 95</p> |

Tabla 5. Matriz DOFA Seguridad de la Información

| MATRIZ DOFA | |
|---|--|
| OPORTUNIDADES | AMENAZAS |
| <ul style="list-style-type: none"> • Fortalecer el Personal técnico de apoyo con capacitaciones. • Fortalecer Equipos de red inalámbrica • Fortalecer las licencias de Software • Implementar antivirus para las estaciones de trabajo • Mejoras en la página web institucional • Fortalecer planes de mejora en la infraestructura de la red IPv4. • Diversidad de equipos y servicios de internet inalámbrico. • Herramienta de trabajo remoto para el servidor de base datos contable. • Garantizar la continuidad del recurso humano complementario de profesionales de apoyo para el soporte técnico para el 2021 • Fortalecer planes de mejora para los sistemas de información • Fortalecer los Backup de la base de datos institucionales. • Garantizar el uso de las buenas prácticas para el uso de las herramientas tecnológicas. • Cumplimiento en la información recibida desde la página web. • Implementar y Fortalecer las UPS para los servidores y estaciones de trabajo • Contar con recursos económicos. • Fortalecer cableado eléctrico. | <ul style="list-style-type: none"> • Falta de soporte de Base de Datos. • Acelerado de las herramientas tecnológicas puede agilizar aún más la obsolescencia de equipos de computo • Sobrecosto por temas de mal uso de los equipos de impresión y por cultura de imprimir todo. • Demora en las contrataciones. • Fallas Definitivas en Servidores • Falta de Antivirus en las estaciones de trabajo. • Ataques a vulnerabilidades. • Falta un plan de contingencia para fallas en la información por virus. • Actividades suspendidas por fallas eléctricas y no contar con una ups que soporte buena capacidad para mantener en funcionamiento las estaciones de trabajo y servidores. • Falta de mantenimiento periódico en los servidores donde se localiza la Base de Datos institucional • Repotenciar y mejorar la configuración y actualización de las estaciones de trabajo. • Repotenciar los servidores. • Pérdida de tiempo del funcionario por mal funcionamientos de la red de datos. • Malas prácticas en el uso de las herramientas tecnológicas. • Sobrecarga eléctrica en las estaciones de trabajo por falta de mantenimiento de la planta eléctrica. • Falta de políticas de seguridad. |

Fuente. Elaboración propia







| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 19 de 95</p> |

Tabla 6. Matriz DOFA Seguridad de la Información (continuación)

| ESTRATEGIA FO | ESTRATEGIA DO |
|---|---|
| <ul style="list-style-type: none"> • Mantener contratado el personal de idóneo de soporte técnico. • Actualizar la infraestructura de red IPv6. • Realización permanente de backUp de base de datos existente. • Actualizar permanentemente la página Web institucional. • Seguimiento y monitoreo de los sistemas de información. • Monitorio permanente de backup de base de datos. • Seguimiento a las buenas prácticas de uso de los sistemas de información. • Actualizar cuando corresponda licencia de software. | <ul style="list-style-type: none"> • Diseñar políticas de seguridad de la información para control riesgos en la entidad. • Sensibilizar el uso de las buenas prácticas en la navegación de internet y uso de herramientas tecnológicas. • Crear un manual de procedimiento en el manejo de los sistemas de información. • Realizar mejoras en el procedimiento de los soporte de mantenimiento de las bases de datos. • Realizar mejoras en el procedimiento del servicio de mantenimiento a las estaciones de trabajo y servidores. • Aplicar seguimiento en la red para el buen funcionamiento y estabilidad de internet y red de datos. • Aplicar políticas de seguridad que permitan controlar los riesgos. • Velar por el correcto funcionamiento de las estaciones de trabajo. • Velar por el buen funcionamiento de los sistemas de información. • Buscar apoyo interno para las capacitaciones en el uso de herramientas tecnológicas. |
| ESTRATEGIA FA | ESTRATEGIA DA |
| <ul style="list-style-type: none"> • Diseñar y Formular las políticas de seguridad orientados al fortalecimiento de la misión de la entidad. • Formular y Socializar la visión estratégica de buenas prácticas para el uso de las herramientas tecnológicas. • Formular estrategias que permitan hacer buen uso del procedimiento de mantenimientos de los equipos de cómputo. • Revisión continúa de las actualizaciones del antivirus en las estaciones de trabajo. • Formular estrategias que mantenga un monitoreado el buen funcionamiento de la red eléctrica. • Mantener el rubro de la contratación del personal para soporte técnico. • Mantener el rubro para las actualizaciones de antivirus y demás herramientas tecnológicas. • Diseñar estrategias de copias de seguridad de manera automática. • Mejoras en el procedimiento de adquisición de los equipos de cómputo y herramientas tecnológicas. | <ul style="list-style-type: none"> • Implementar las políticas de seguridad orientados al fortalecimiento de la misión de la entidad. • Elaborar el plan de fortalecimiento de la página web institucional. • Capacitar el recurso humano para las buenas prácticas para el uso de las herramientas tecnológicas. • Manejo adecuado de las backUp de bases de datos institucionales. • Implementar plan de contingencias para los activos de la información. • Implementar un sistema para el manejo de los correos electrónicos de la entidad. • Implementar un sistema para la organización de archivos digitales e institucionales. • Sensibilizar al recurso humano de las sanciones por el mal uso de las políticas de seguridad. • Implementar un plan a los equipos que no tengan protección y configuración de seguridad. |

Fuente. Elaboración propia





| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 20 de 95</p> |

Teniendo en cuenta lo anterior, se deben establecer estrategias de seguridad de la información acorde con los objetivos estratégicos de la Entidad, en donde desde la Dirección se plantea:

- **Planeación:** Definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados con la misión, visión, funciones de la Institución y objetivos estratégicos.
- **Normalizar.** Estandarizar las acciones y actividades cotidianas para el uso adecuado de las tecnologías y sistemas de información:
 - Uso adecuado de estaciones de trabajo
 - Uso de equipos portátiles
 - Uso de recursos de red
 - Controles de Acceso
 - Uso de software
 - Uso de unidades de almacenamiento
 - Uso de correos electrónicos
- **Implementación:** Disponer del equipo que lleve a cabo la planeación, ejecución y seguimiento de las acciones definidas.
- **Cultura organizacional:** Dar a conocer y recalcar que la información que reside en cada PC o medio de almacenamiento auxiliar (DVD, USB, Disco externo etc.) es responsabilidad de cada usuario, para que no sean desconocedores del riesgo que se toma cuando no se tiene un uso debido de la tecnología y a la vez de los sistemas de información; especialmente, con contenidos de internet que tenga extensiones maliciosas de navegador que pueden ser una fuente importante de filtración de datos y de fraudes por ejemplo, las cuentas bancarias, registro de datos de usuarios e información.



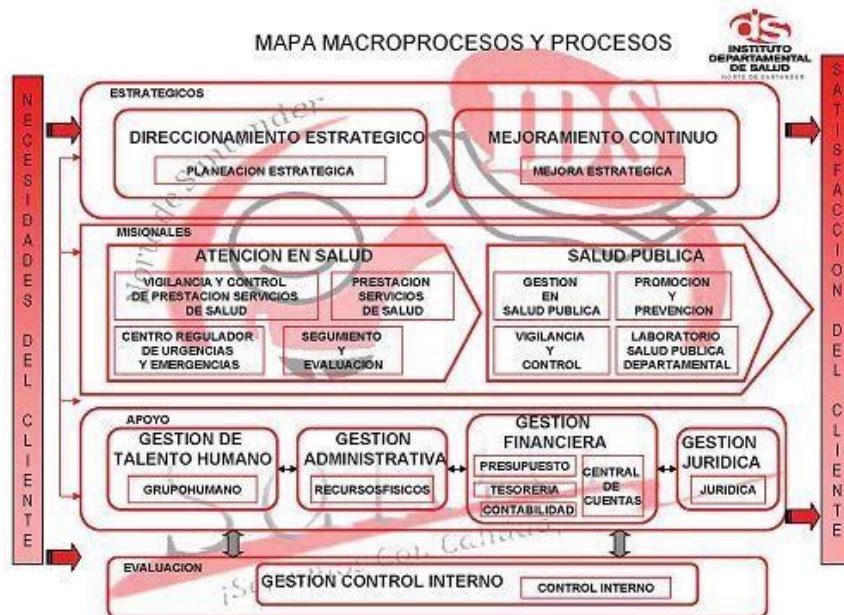
| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 21 de 95</p> |

- Mejoramamiento Continuo. Mantener en retroalimentación el Sistema de Gestión de Seguridad de la Información de manera que contribuya a la eficiencia, eficacia y efectividad de la Entidad.

3. POLÍTICAS DE SEGURIDAD



El proceso escogido fue Planeación Estratégica, en donde se encuentra las Tecnologías de la Información y las Comunicaciones que se encuentra inmerso dentro del macro proceso Direccionamiento Estratégico del Instituto Departamental de Salud de Norte de Santander.

Ilustración 3 Mapa de Macroprocesos y Procesos del IDS



Fuente. Tomado de Sistema Integrado de Gestión (IDS, 2021)



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 22 de 95</p> |

El propósito principal del macroproceso es organizar el desarrollo y ejecución de los objetivos institucionales mediante la formulación de planes que orienten a las áreas estratégicas de la institución de la realización de las metas misionales en cumplimiento de los lineamientos nacionales en salud.

A su vez el proceso escogido tiene como propósito apoyar el correcto funcionamiento de los recursos tecnológicos para el desarrollo de las funciones de las diferentes áreas de la entidad, esto con el fin de lograr el alcance de los objetivos propuestos por el IDS, garantizando la prestación de los servicios con calidad que satisfagan las necesidades de los usuarios del sistema de salud del departamento Norte de Santander.



3.1. Política general de seguridad

3.1.1 Introducción

Las tecnologías y sistemas de información permanece en continua evolución, lo que conlleva una mayor responsabilidad en su manejo, teniendo en cuenta que las amenazas también se encuentra en proceso continuo de expansión, presentándose cada día mayores riesgos, vulnerando la estabilidad de la infraestructura tecnológica.

Con el transcurrir de los años, en el Instituto Departamental de Salud de Norte de Santander las operaciones institucionales se han incrementado, lo que ha trascendido en la adquisición de tecnologías y sistemas de información que facilite el quehacer diario. En la actualidad, el Instituto cuenta con una gran talento humano, distribuidos en dependencias, grupos y subgrupos, quienes tienen asignados equipos informáticos y sistemas de información, que se utilizan diariamente de manera ardua, por tal razón, surge la necesidad de establecer políticas generales de seguridad que



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 23 de 95</p> |

inviten a cada uno de sus funcionarios a “reconocer la información como uno de sus principales activos” (Cano) y por tal razón aplicarlas para perseverar y conservarlo.

De acuerdo a lo descrito por Cano (2000) se definió para ésta política 6 elementos fundamentales, los cuales estaban contemplados en la Política de seguridad de la información de la Secretaria Distrital De Salud de Bogotá (2012). Para unificar criterios también se analizó la Política General de Seguridad de la Información de la Comisión Nacional de Investigación Científica y Tecnológica (2011) y la Política de seguridad de la información de Invima (2017) que sirvieron como marco teórico para la definición de ésta política.



3.1.2 Objetivo General

Determinar los lineamientos que permitan garantizar que la plataforma tecnológica de la IDS (recursos de software, recursos de hardware y sistemas de información) se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto, cumpliendo las normas y políticas de seguridad de la información.

3.1.3 Objetivos Específicos

- Proponer los mecanismos de seguridad lógica, en el ambiente informático de modo que se contribuya con la confidencialidad, integridad y disponibilidad de la información.
- Garantizar que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 24 de 95</p> |

- Garantizar la exactitud y completitud de la información garantizando que la información sea precisa, coherente y completa desde su creación hasta su destrucción.
- Garantizar que la información sea accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está.
- Asegurar que sólo los individuos autorizados tengan acceso a los recursos.
- Disminuir las amenazas a la seguridad de la información y los datos.
- Evitar el comportamiento inescrupuloso y uso indiscriminado de los recursos.
- Cuidar y proteger los recursos tecnológicos del IDS.
- Concientizar a la comunidad sobre la importancia del uso racional y seguro de la infraestructura informática, sistemas de información, servicios de red y canales de comunicación.
- Promover las mejores prácticas de seguridad física, mediante la implementación de ambientes adecuados que permitan la correcta custodia de los datos y equipos para poder así utilizar de manera eficiente de los recursos de tecnologías de información.



3.1.4 Alcance

Esta política se aplica a todas las personas (Funcionarios, Contratistas y personal externo que preste servicios remunerados o no al IDS), que tienen acceso a la información, recursos y servicios informáticos.

3.1.5 Política

Uso de la información.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 25 de 95</p> |

La oficina de Sistemas de Información, como administrador de la plataforma tecnológica y generador de la política general de seguridad del IDS, garantiza la adecuada gestión de la seguridad de la información procesada y/o que alberga por los sistemas y servicios contemplados en el alcance.

Toda la información que es generada por los funcionarios, contratistas y practicantes del IDS en beneficio y desarrollo de las actividades propias del Instituto es propiedad del IDS, a menos que se acuerde lo contrario en los contratos escritos y autorizados. Esto también incluye la información que pueda ser adquirida o cedida a la Institución de parte de entidades o fuentes externas de información que sean contratadas o que tengan alguna relación con la Institución.



El IDS protege la información creada, procesada, transmitida o resguardada por los procesos de su competencia, su infraestructura tecnológica y activos, del riesgo que se genera con los accesos otorgados a terceros (ej.: contratistas, proveedores o ciudadanos), o como resultado de servicios internos en outsourcing.

Las responsabilidades frente a la seguridad de la información del Instituto son definidas, compartidas, publicadas y deberán ser aceptadas por cada uno de los funcionarios, contratistas o practicantes del Instituto.

Uso de control de acceso

Expone las condiciones, normas y procedimientos necesarios para fijar los requisitos que se deben cumplir por cualquier funcionario, contratista o practicante del Instituto para obtener acceso a los sistemas de información, hardware y software propiedad de la institución.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 26 de 95</p> |

La oficina de Sistemas de Información, puede acceder e inspeccionar, sin necesidad de previo aviso, todos los dispositivos informáticos propiedad del IDS, conectados o no a la red y de los recursos de software, para los propósitos de resolución de problemas o para investigar violaciones a las políticas, normas y procedimientos definidos por la entidad.

El IDS implementa control de acceso a la información, aplicativos, recursos de red, portales y sistemas de información internos y externos o con accesos remotos.

El IDS garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

La oficina de Sistemas de Información, es el único autorizado para ingresar a la red de la IDS, nuevos recursos y sistemas informáticos (Software, hardware, seguridad, equipos de red etc.).



Uso de dispositivos de almacenamiento de información

Describe el uso permitido de los dispositivos de almacenamiento externo en el IDS y las restricciones en su empleo al interior de la institución.

Cada usuario, deberá velar por el cumplimiento de las políticas de uso de unidades de almacenamiento de información de su dependencia (donde labora), estipulando mecanismos y tiempos para la realización de copias de respaldo de su estación de trabajo, controlando la efectividad de este procedimiento.

El IDS, se compromete a salvaguardar la información que genera en la ejecución de sus funciones o la que le es entregada en custodia por usuarios dentro de la ejecución de los trámites del instituto.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 27 de 95</p> |

Uso de estaciones de trabajo

Define los mecanismos necesarios que se deben aplicar en el Instituto con el fin de proteger la información física residente en los puestos de trabajo y la información digital almacenada en cada uno de ellos e infraestructura técnica a disposición de todos los funcionarios, contratistas o practicantes para el normal desarrollo de las actividades.

El uso o conexión a los recursos y servicios de TI de la Red del IDS, implica el total conocimiento y aceptación de las normas y políticas que regulan el uso de estos recursos, al ingresar a la Red, el usuario asume toda responsabilidad legal que surja de una violación a estas políticas.



Desarrollar todas las medidas necesarias para garantizar la adecuada gestión de los incidentes de seguridad que puedan producirse, y que permitan la resolución tanto de las incidencias menores como de las situaciones que puedan poner en riesgo la continuidad de las actividades contempladas.

Toda persona que use o acceda a los recursos o servicios de TIC de la SDS, deberá utilizarlo para los fines destinados a contribuir al cumplimiento de los objetivos del IDS, para el cumplimiento de esta política, se obliga a todo el personal (Funcionarios y Contratistas), a solicitar autorización previa por parte del jefe inmediato.

Todo el personal del IDS, (Funcionarios y Contratistas) será responsable civil y penalmente, por la mala utilización de la información reservada.

Los dispositivos y sistemas conectados a la Red en todo momento, deben contar con las licencias de software, conforme a las leyes que regulan la materia.



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 28 de 95</p> |

Todos los PC, que se conecten en red interna del IDS, deberán tener instalado en forma permanente y actualizada un antivirus activo.

A criterio de la oficina de SI, aquellos equipos, sistemas, software utilitario que puedan calificarse como riesgosos para la entidad o para los datos que tiene la entidad, o para los sistemas o los servicios de TIC, serán desconectados de la red, sin aviso previo.

Uso del servicio de correo electrónico

Concientiza a los funcionarios, contratistas o practicantes de la Institución de los riesgos asociados con el uso de correo electrónico y presenta las normas y protocolos a seguir para del correo institucional.

Uso del servicio de internet / intranet



Concientiza a los funcionarios, contratistas o practicantes de la Institución de las buenas prácticas a seguir sobre las normas de uso del servicio de Internet/Intranet, así como el conocimiento de los riesgos asociados por el uso indebido de los mismos.

Mantenimiento y definición de la política

Destinar los recursos y medios necesarios para desarrollar todas las medidas de seguridad que se determinen, manteniendo un adecuado balance entre costo y beneficio.

Establecer un plan de formación y concientización en materia de seguridad de la información que ayude a todo el personal implicado a conocer y cumplir las medidas de seguridad establecidas y a participar de forma proactiva en la gestión de la seguridad de la información.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 29 de 95</p> |

Definir e implantar un Proceso de Continuidad orientado a proteger los servicios y procesos de TIC de la entidad.

Las políticas de seguridad general para el IDS, prevalecen sobre los requerimientos individuales y cualquier eventualidad de excepción a los mismos deberá ser analizada. En caso de ser necesario se llevará al “Comité de seguridad” quien definirá o no su aplicación.

Debe existir un comité de seguridad de la información encargado de establecer los procedimientos y formas de actuación necesarias para garantizar el correcto desarrollo de esta política, que se plasman en un sistema de seguridad, documentado y conocido por todo el personal del IDS.

La oficina de SI será la responsable de coordinar la reparación y mantenimiento de equipos, las reparaciones y/o ampliaciones de estos equipos no pueden ser hechas o contratadas por ningún usuario diferente a los funcionarios o contratistas del IDS.



La administración de toda la plataforma tecnológica del IDS, es responsabilidad de la oficina de SI.

A este documento podrán integrarse en adelante lineamientos o políticas relativas.

Aplicación de la Política y responsabilidades

La presente Política General de Seguridad de la Información entra en vigencia una vez oficializada por el Director del IDS y las coordinaciones de los distintos Grupos, Subgrupos y dependencias serán responsables de ponerlas en conocimiento de su personal subordinado y demás personas.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 30 de 95</p> |

Para el caso del personal que se contrate con posterioridad a la fecha de publicación, se le deberá entregar una copia del presente documento y hacer firmar una declaración de toma de conocimiento y aceptación de la misma.

Director del IDS: en su calidad de tal, responde ante la Junta Directiva la existencia y cumplimiento de las medidas que mantengan un nivel de seguridad de la información acorde con el rol de la organización y los recursos disponibles.

Encargado de la oficina de Sistemas de Información: es el principal responsable en la definición de los criterios de seguridad de la información en IDS, para lo cual deberá analizar periódicamente el nivel de riesgo existente, proponiendo soluciones. Una vez autorizada la implementación de las medidas, deberá coordinar con quienes corresponda su materialización oportuna y correcta.

Comité de Seguridad: tiene por responsabilidad ser la instancia orientadora de la implementación de la política de seguridad del IDS y asesorar al Director, en temas de seguridad de la información, en coordinación con el Encargado de Sistemas de Información.



Personal de IDS: tiene la responsabilidad de cumplir con lo formalizado en este documento y aplicarlo en su entorno laboral. Además, tiene la obligación de alertar de manera oportuna y adecuada, cualquier incidente que atente contra la seguridad de la información.

Violaciones y sanciones.

De acuerdo al Código Disciplinario Único – Ley 734 (2014) Artículo 34, como servidor público se tiene deberes entre los cuáles se encuentran:

- “Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que



| | | |
|--|-------------------------------------|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 31 de 95</p> |

tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos”

- “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, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos”
- “Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización”

Teniendo en cuenta lo anteriormente expuesto, el incumplimiento de esta política, podrá incurrir en una falta disciplinaria. Según la gravedad que se cometa se estandariza tres niveles: leves, graves y gravísimas.

Cuando se determine que la falta es por primera vez por desconocimiento y no afectó al bien, recurso ni documentación no afecte, son faltas leves dando lugar a una **Amonestación Verbal**, sin embargo, si se determina lo contrario que son faltas graves o gravísimas se traslada por escrito a la Oficina de Recursos Humanos cuya comisión determinará si da lugar a una **Amonestación Escrita** a la hoja de vida según como lo establece en el Código Disciplinario Único – Ley 734 (2014).



En cualquier caso de amonestación verbal o escrita y en el caso que lo amerite, el funcionario deberá resarcir el daño o devolver, restituir o reparar el bien afectado.

3.2 Política particular para el uso adecuado de estaciones de trabajo

3.2.1 Objetivo

Establecer las directrices para garantizar el uso adecuado de las estaciones de trabajo.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 32 de 95</p> |

3.2.2 Alcance

Esta política se aplica a todas las personas (Funcionarios, Contratistas y personal externo que preste servicios remunerados o no al IDS), que tienen acceso a la información, recursos y servicios informáticos.

3.2.3 Responsabilidades

Funcionario: Toda persona de planta o contratistas y personal externo que preste servicios remunerados o no al IDS, deberá cumplir con lo pactado en esta política.



Oficina de sistemas de información: Velar por la efectividad de esta política, brindando asesorías y adiestramientos al personal para el uso de las herramientas informáticas.

Oficina de Recursos Humanos: Velar por el cumplimiento de esta política y que todo el personal esté capacitado y la conozca, además de aplicar las sanciones que requiera al incumplimiento de la misma.

3.2.4 Violaciones y Sanciones

El incumplimiento de esta política, incurrirá en una falta disciplinaria cuya comisión da lugar a una **Amonestación Verbal** y si es reiterativa se traslada por escrito a la Oficina de Recursos Humanos cuya comisión determinará si da lugar a una **Amonestación Escrita** a la hoja de vida según como lo establece en el Código Disciplinario Único – Ley 734 (2014).



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 33 de 95</p> |

3.2.5 Política

El Instituto Departamental de Salud de Norte de Santander asigna a los funcionarios en apoyo al cumplimiento de sus labores, cuando así se requiere una estación de trabajo. Estos equipos son parte del patrimonio institucional, por tanto, se debe buscar la mejor forma de utilizarlos, tomando en cuenta aspectos de seguridad físicos y lógicos para su protección, finalmente, la aplicación de las mejores prácticas de uso de las estaciones para proteger el equipo y la información contenida en él.

Instalación de Equipos



Los equipos de cómputo (computadores, sitios de trabajo, servidores y demás equipos) deben tener una instalación por parte de un funcionario de la oficina de SI para que la instalación sea adecuada concorde con cada una de las diferentes partes así como las partes eléctricas, por ejemplo, los estabilizadores no deben estar cerca de la pantalla y los dispositivos de computo siempre deben estar sobre las superficies de trabajo, para que el manejo y control del equipo sea el mejor.

Los equipos deben estar ubicados en sitios adecuados, evitando la exposición al sol, al polvo o zonas que generen electricidad estática.

No se puede instalar ni conectar dispositivos o partes diferentes a las entregadas en los equipos. Es competencia de la oficina de sistemas de información el retiro o cambio de partes y/o componentes.

Los equipos, escáner, impresoras, lectoras y demás dispositivos, no podrán ser trasladados del sitio que se les asignó inicialmente, en el caso de ser necesario, debe



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 34 de 95</p> |

ser notificado tanto a Almacén como a la oficina de Sistemas de Información para su respectivo control.

Se debe garantizar la estabilidad y buen funcionamiento de las instalaciones eléctricas, asegurando que los equipos estén conectados a las instalaciones eléctricas apropiadas de corriente regulada, fase, neutro y polo a tierra.

La oficina de Sistemas de Información debe realizar la hoja de vida de los equipos de cómputo para llevar un control de los equipos propiedad del Instituto, en donde se manifieste el usuario que tenga asignado el equipo bajo su responsabilidad.

La oficina de Sistemas de Información deberá especificar las características necesarias para la adquisición de equipos de acuerdo a su operación y funcionamiento.



Al responsable del equipo se le asigna un usuario con la respectiva contraseña, independiente del usuario administrador que ejerce control sobre las configuraciones específicas del equipo.

Manipulación de Equipos

La infraestructura tecnológica (servidores, computadores, impresoras, UPS, escáner, lectoras y equipos en general) no puede ser utilizado en funciones diferentes a las institucionales.

Ningún funcionario a excepción de la oficina de Sistemas de Información se encuentra autorizado para manipular los componentes de los equipos de cómputo.



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 35 de 95</p> |

El equipo que ha sido asignado al usuario es de su responsabilidad la manipulación y acceso al equipo para conservar el activo físico como se le ha sido asignado.

La manipulación, daños y partes faltantes son de responsabilidad del usuario a quien se le asignó el equipo, quien deberá controlar el acceso a las demás personas no autorizadas debido a que el equipo está a su cargo.

Los equipos deben ser manipulados de tal manera que cumplan y satisfagan las tareas a las cuales fueron designados debido a cada una de las funciones y programas instalados, con el fin de realizar el cumplimiento de las actividades designadas por su dependencia.

Los equipos deben ser manipulados de la forma en la que se encuentra situadas sus partes con el fin de que no existan fallas tanto eléctricas como funcionales debido a los movimientos bruscos o por la ubicación incorrecta de sus partes.



La manipulación de los equipos también incluye la revisión de los equipos con fallas causadas por la mala conexión o falta de conexión eléctrica que puede ser realizada por los mismos usuarios sin hacer solicitud a la oficina de sistemas de información.

La utilización de los equipos es con fin de trabajo; no se pueden realizar descargas de otra serie de software ajeno a las actividades informáticas de la oficina.

No es permitido destapar o retirar la tapa de los equipos, ni podrá retirar o instalar partes sin la autorización de la Oficina de sistemas de información.

Ningún funcionario podrá formatear los discos duros de los computadores, sin previa autorización de la oficina de sistemas de información.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 36 de 95</p> |

Antes de desconectar cualquier dispositivo del computador se debe desconectar previamente del equipo, en caso contrario, se puede perder datos, o incluso dañar el dispositivo, haciendo inaccesible todo el contenido.

No es recomendable guardar ningún dispositivo de almacenamiento magnético de información cerca de ninguna fuente electromagnética, como altavoces, transformadores, etc.

Buenas Prácticas Frente a un Computador

Mantener limpio de polvo el computador y libre de otros objetos, de modo que no se obstruya ningún punto de ventilación, pues a través de las ranuras de la CPU capta el aire del exterior para la refrigeración de los distintos componentes. Igualmente, se debe tener la prevención con los periféricos.



Por seguridad en el lugar de trabajo, la espalda debe estar recta y los pies apoyados en el suelo, con el fin de prevenir problemas en la columna.

Mantener los codos con un ángulo de 90 grados del teclado y mouse para que las muñecas no estén flexionadas y apoyadas para evitar dolores en las articulaciones de la mano y futuras complicaciones.

No comer, fumar ni ingerir líquidos frente el computador para evitar incidentes y accidentes, además, por su salud se evita adquirir bacterias y en algunos casos prevenir la obesidad.

Mantener una distancia mínima de 55 cm de la pantalla y los ojos deben estar a la misma altura que el borde superior de la pantalla con el fin de prevenir cansancio en los ojos, posible problemas con la visión, dolores de cabeza, espalda o cuello.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 37 de 95</p> |

No golpear ni mover bruscamente los equipos ni sus periféricos.

Se aconseja utilizar colores claros y mate en la pantalla para evitar cansancio en la vista.

La posición del monitor debe evitar que la luz incida directamente sobre la pantalla para prevenir daños a causa del reflejo de la misma y, al mismo tiempo, evitar una visualización incómoda.

Evitar limpiar la pantalla con productos que puedan dañarla como alcohol o jabones, se aconseja usar un trapo de tela suave ligeramente humedecido y no hacer fuerza excesiva durante la limpieza.

En el caso de personas zurdas han de cambiar la posición del ratón al lado izquierdo del teclado y configurarlo así en las propiedades del ratón desde el Panel de Control.

Mantener los equipos apagados mientras no se estén utilizando.



Mantenimiento de Equipos

La conservación de los equipos, su funcionamiento, la seguridad física de cada equipo hacen parte de las responsabilidades de los usuarios.

La instalación de cada uno de los equipos conforme al sitio y espacio de trabajo, el mantenimiento preventivo y correctivo es responsabilidad de la Oficina Sistemas de Información.

Está prohibido que los equipos informáticos sean atendidos por personal ajeno a la Oficina de Sistemas de Información para el mantenimiento preventivo y correctivo. El



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 38 de 95</p> |

funcionario responsable del equipo responderá por daños adversos a estos mantenimientos o arreglos realizados por terceros.

Los usuarios también hacen parte del mantenimiento de los equipos de cómputo haciendo un buen uso y utilidad de los equipos para que su funcionamiento sea el mejor y los manteamientos preventivos y correctivos se prolonguen con la ayuda de la buena manipulación.

Los responsables de cada una de las dependencias, grupos y subgrupos pueden hacer una solicitud a Sistemas de Información en el formato respectivo de mantenimiento correctivo desde el momento que el equipo este fallando y las precauciones realizadas por el usuario no hayan sido satisfactorias para que el equipo funcionara.



Las solicitudes de mantenimientos externos a equipos del Instituto son determinadas por la Oficina de Sistemas de Información con un previo análisis de funcionamiento, con el fin de dar a conocer que el mantenimiento o arreglo se debe realizar externamente.

Es estrictamente obligatorio, informar oportunamente al departamento de sistemas la ocurrencia de novedades por problemas técnicos, eléctricos, de planta física, líneas telefónicas, o cualquiera otra, que altere la correcta funcionalidad.

Queda rotundamente prohibido realizar mantenimiento preventivo y correctivo a equipos ajenos al Instituto.

Actualización de Equipos



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 39 de 95</p> |

Los equipos de cómputo (computadores, sitios de trabajo, servidores y demás equipos), y equipos de red que sean propiedad del Instituto Departamental de Salud se debe actualizar de manera periódica manteniendo las funcionalidades necesarias por el usuario, con el fin de aumentar la calidad de servicio, actividades y atención por cada uno de los usuarios y responsables de los equipos, aumentando su desempeño.

3.3 Política particular para el control de acceso

3.3.1 Objetivo

Establecer las directrices para controlar el acceso a equipos informáticos, red de datos institucional y documentación institucional.



3.3.2 Alcance

Esta política se aplica a todas las personas (Funcionarios, Contratistas y personal externo que preste servicios remunerados o no al IDS), que tienen acceso a la información, recursos y servicios informáticos.

3.3.3 Responsabilidades

Funcionario: Toda persona de planta o contratistas y personal externo que preste servicios remunerados o no al IDS, deberá cumplir con lo pactado en esta política.



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 40 de 95</p> |

Oficina de sistemas de información: Velar por la efectividad de esta política, brindando asesorías y adiestramientos al personal para el uso de las herramientas informáticas.

Oficina de Recursos Humanos: Velar por el cumplimiento de esta política y que todo el personal esté capacitado y la conozca, además de aplicar las sanciones que requiera al incumplimiento de la misma.



3.3.4 Violaciones y sanciones

El incumplimiento de esta política, incurrirá en una falta disciplinaria cuya comisión da lugar a una **Amonestación Verbal** y si es reiterativa se traslada por escrito a la Oficina de Recursos Humanos cuya comisión determinará si da lugar a una **Amonestación Escrita** a la hoja de vida según como lo establece en el Código Disciplinario Único – Ley 734 (2014).

3.3.5 Política

El Instituto Departamental de Salud de Norte de Santander asigna a cada funcionario en apoyo al cumplimiento de sus labores dando acceso a equipos informáticos, a la red de datos institucional y a documentación, con la cual el empleado puede acceder diferentes elementos que la componen como: servidores de archivos, servidores de bases de datos, impresoras, archivos compartidos en otras estaciones de trabajo, sistemas y aplicaciones Institucionales, entre otros. Por lo anterior, los empleados deben hacer uso de la red y de los servicios relacionados con esta, estrictamente en cumplimiento de las labores institucionales, tomando en consideración la privacidad de otros usuarios y la no saturación de la red por uso indebido del ancho de banda.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 41 de 95</p> |

Control de Acceso a Equipos Informáticos

Todos los equipos de cómputo tienen asignado un responsable y un usuario, debe cumplir con la responsabilidad de darle buen uso y funcionamiento a los equipos.

Los equipos de cómputo que se encuentren en áreas críticas donde sea de fácil acceso deben tener un seguimiento y deben poseer su respectiva seguridad.

Los cuartos de Rack son áreas donde se encuentren los equipos imprescindibles para el funcionamiento y trabajo en los departamentos del instituto, el cual, se encuentra restringido el acceso a los funcionarios ajenos a la Oficina de Sistemas de Información.

El servidor de datos, es para almacenamiento de documentos institucionales, estos archivos deben ser productos de las funciones del personal o sirvan como apoyo para la ejecución de dichas funciones.



Las impresoras no son para uso personal, se prohíbe la impresión total o parcial de información ajena al Instituto Departamental de Salud.

Los equipos con acceso a la red institucional e internet no podrán usar el ancho de banda para ver videos, escuchar música o acceder a redes sociales, ya que el uso del internet es estrictamente necesario para cumplir las labores del cargo.

Las diversas páginas web que funcionan como redes sociales, tienen contenido de video, música o contenido para adulto, están estrictamente restringidas.

Está restringido el uso de programas de descarga de contenido audiovisual (música, videos, fotos) y software, que no apoye desarrollo de las funciones laborales para cumplir la misión de la institución.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 42 de 95</p> |

Control de Acceso a la Red Local

La Oficina de Sistemas de Información es responsable de dar acceso a un punto remoto, en el cual es asignada una dirección IP dentro del rango de direcciones que el instituto tiene para ofrecer conectividad a internet y recursos compartidos.

Los usuarios deben hacer utilización de la red local de manera adecuada (no acceder a información ajena y no utilizar recursos de red que no estén permitidos) para que el funcionamiento y la realización de las tareas sean las mejores.



La Oficina de Sistemas de Información es el encargado de visualizar y realizar prevención del buen uso de la red.

El acceso a los equipos de cómputo especializados como servidores y equipos de red se debe hacer por medio del personal autorizado por la Oficina de Sistemas de Información.

Los equipos que son del instituto y sean conectados a la red local, o aquellos que sean conectados a la red inalámbrica deben hacer uso de la misma de manera responsable y con la mejor de las disposiciones para el buen funcionamiento de las redes.

El acceso a la red institucional deberá realizarse por medio del dominio IDS con su respectivo usuario y contraseña, los cuales son asignados por el área de sistemas a cada equipo teniendo en cuenta el procedimiento de Ingreso de un nuevo equipo a la red institucional.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 43 de 95</p> |

Los equipos personales que requieran el acceso a la red institucional, debe ser solicitado a la Oficina de Sistemas de Información por medio del formato de solicitud de servicio interno.

Control de acceso a la documentación

El control de acceso a la documentación que es compartida en red se debe hacer de manera segura y con precauciones de guardar una copia en el equipo del usuario.

La documentación que se encuentre en red se debe compartir con los usuarios beneficiados con la documentación la cual hace parte de sus actividades de trabajo con la restricción de acceso a personas ajenas a las actividades que en esta documentación se emplean.



La información que se encuentre en la red se debe proteger y utilizar solo con fines laborales, no con fines de lucrarse haciendo mala utilización de la documentación o siendo transferida a terceros, los cuales harán utilización de información con otros fines de dañar la institución.

3.4 Política particular para el uso de Dispositivos de Almacenamiento de Información

3.4.1 Objetivo

Establecer las pautas para regular el uso de cualquier tipo de unidades de respaldo, entre las que podemos mencionar los quemadores de discos compactos, DVD,



| | | |
|--|-------------------------------------|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 44 de 95</p> |

memorias USB, Disco Duros interno y externos entre otros; con el objeto de que su uso sea para labores propias de la institución.

3.4.2 Alcance

Esta política se aplica a todas las personas (Funcionarios, Contratistas y personal externo que preste servicios remunerados o no al IDS), que tienen acceso a la información, recursos y servicios informáticos.

3.4.3 Responsabilidades

Funcionario: Toda persona de planta o contratistas y personal externo que preste servicios remunerados o no al IDS, deberá cumplir con lo pactado en esta política.



Oficina de sistemas de información: Velar por la efectividad de esta política, brindando asesorías y adiestramientos al personal para el uso de las herramientas informáticas.

Oficina de Recursos Humanos: Velar por el cumplimiento de esta política y que todo el personal esté capacitado y la conozca, además de aplicar las sanciones que requiera al incumplimiento de la misma.

3.4.4 Violaciones y sanciones

El incumplimiento de esta política, incurrirá en una falta disciplinaria cuya comisión da lugar a una **Amonestación Verbal** y si es reiterativa se traslada por escrito a la Oficina de Recursos Humanos cuya comisión determinará si da lugar a una **Amonestación**



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 45 de 95</p> |

Escrita a la hoja de vida según como lo establece en el Código Disciplinario Único – Ley 734 (2014).

3.4.5 Política

Teniendo en cuenta la importancia de la información que maneja el Instituto Departamental de Salud de Norte de Santander y la necesidad de resguardar los datos, así como emitir información a otras entidades, surge la necesidad de establecer que toda unidad que cuente con dispositivos para la realización de respaldos (computadoras de escritorio, portátiles y servidores) debe velar porque se haga un uso adecuado de esos recursos, utilizándolos únicamente para cumplir con los intereses de la institución, y tomando en cuenta las funcionalidades operativas del equipo.

Buenas Prácticas

No se permite realizar copia no autorizada de material protegido por derecho de autor.



No se permite almacenar información de índole personal como videos, fotos, música entre otros, en los equipos institucionales ni equipos servidores.

No se permite modificar, eliminar o copiar un archivo perteneciente a otro Usuario sin el previo consentimiento del dueño del archivo.

Todo archivo de índole personal que se encuentre en el servidor de datos, será borrado inmediatamente sin previa autorización.

Organización de la Información en un Equipo de Cómputo



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 46 de 95</p> |

Sistemas de Información debe crear en los computadores dos particiones. La primera corresponderá al lugar en el cual se instalará el Sistema Operativo, la segunda corresponderá al lugar en el cual se guardará la información del usuario, aunque esto no garantiza la permanencia de la información ni tampoco sea una regla que se deba tener en los computadores, si se facilitan las cosas a la hora de hacer una restauración del computador por daño en el Sistema Operativo

El usuario debe guardar toda la información generada en la partición creada por la Oficina de Sistemas de Información, en dado caso, que el equipo no cuente con dicha partición, el usuario deberá crear una carpeta con el nombre del equipo, en el disco local C y guardar toda la información en dicha carpeta.



Nombre de los Archivos

Se recomienda no guardar archivos con nombres muy largos. Es de vital importancia a la hora de realizar una copia de seguridad, pues en ocasiones, los archivos que tienen nombres muy largos ocasionan problemas y no permiten su manipulación.

Es importante nombrar los archivos con nombres que permitan reconocer el contenido. Con el fin de evitar la revisión de todos los archivos que están en el computador abriéndolos, sino que simplemente se pueda limitar a leer el nombre del archivo, y con esto tomar la decisión si se guarda o se elimina.

Tener en cuenta que algunos Sistemas Operativos no permiten ingresar unos caracteres especiales al nombre del archivo, por tanto, se sugiere no nombrar archivos o carpetas utilizando caracteres especiales como (#\$%&?'|¿).



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 47 de 95</p> |



Organización de los Archivos

Se recomienda llevar control y orden de los archivos, con el fin de aprovechar el espacio del equipo de cómputo y facilitar la búsqueda de información.

No se recomienda crear demasiadas subcarpetas, ya que al momento de realizar copias de seguridad el sistema operativo incluye la ruta del archivo como si formara parte del nombre del archivo.

Grabar cambios de archivos frecuentemente. Al trabajar con documentos de texto, planillas de cálculo u otro archivo, se recomienda guardar los cambios frecuentemente para evitar pérdida de los avances frente a un apagado inesperado del equipo. En lo posible, utilizar versiones de los archivos en la medida que se generan modificaciones en ellos.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 48 de 95</p> |



4. INFORME DE ANÁLISIS DE LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

La información en la actualidad juega un papel importante en las organizaciones, es así que varios autores dan gran importancia a la información en sus escritos, Davenport Prusak la define como “un conjunto de datos procesados y que tienen un significado (relevancia, propósito y contexto), y que por lo tanto son de utilidad para quién debe tomar decisiones, al disminuir su incertidumbre” citado por (Sinnexus, 2017), otro aporte importante es el que escribe (Rivas Fernández, 2003) “la información debe ser vista como otro recurso de toda organización igualmente importante que traspasa las fronteras de todo proceso administrativo”.

De acuerdo a lo anterior, es necesario salvaguardar y proteger la información que produce, procesa y almacena el Instituto Departamental de Salud, como activo fundamental para el diseño de estrategias que permitan el fortalecimiento y mejoramiento continuo del proceso de salud pública en el departamento y contribuya al desarrollo de sus funciones como ente de dirección Departamental.

La metodología usada para realizar el análisis de Riesgos al proceso de Planeación estrategia se compone en cuatro pilares: activos de información, amenazas, controles y estimación de riesgos, que son los componentes del estudio descritos a continuación, según Magerit versión 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (2012).



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 49 de 95</p> |

4.1 Caracterización de los Activos de Información

En este apartado se identifican los activos de información que hacen parte del proceso **TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES**, la dependencia entre ellos y se determina el valor.



Los activos de información procesan, generan, transfieren o recogen información; Se define activo de información como “todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección” según la norma ISO 27000:2013 citado por (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016), la identificación de activos nos proporciona información suficiente para la valoración de los riesgos, basados en la metodología de Magerit 3.0 libro 1, encontramos otra definición de activo indicando que es un “componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008]” citado por (Ministerio de Hacienda y Administraciones Públicas, 2012).

Activos de Información a todos aquellos recursos de valor para una organización que generan, procesan, almacenan o transmiten información.

Para la identificación de los activos se realizó un proceso de recolección de información a través de mesas de trabajo con los funcionarios y contratistas de la oficina de planeación y sistemas de información, de las cuales salieron dos tipos de activos:

- Datos e información: Son las aplicaciones informáticas como él (software) materializan la información que permite manejar los datos.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 50 de 95</p> |

- **Sistemas e Infraestructura:** son los equipos informáticos como él (hardware) y que permiten hospedar datos, aplicaciones y servicios. Los soportes de información: que son dispositivos de almacenamiento de datos.

4.2 Valoración de Activos

Como lo indica (Ministerio de Hacienda y Administraciones Públicas, 2012) “La valoración se puede ver desde la perspectiva de la ‘necesidad de proteger’ pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes, La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles)”.

Se identifica que los activos se deben valorar con el objetivo asegurar que la información reciba los niveles de protección adecuados, ya que con base en su valor y de acuerdo a otras características particulares requiere un tipo de manejo especial (2016). La valoración de activos de información que hacen parte del proceso **Tecnologías de la Información y las Comunicaciones**, se realiza de manera cualitativa, el instituto departamental de salud no tiene cuantificado dicho valores.

Para determinar la magnitud de daño se estableció una tabla de valores que permita estandarizar valores que permita comparar, una escala logarítmica y con un criterio homogéneo (Gobierno de España, 2012). Para el análisis del impacto en los activos de información del proceso escogido se definieron cuatro categorías las cuales están definidas y especificadas en la siguiente tabla.







| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 51 de 95</p> |

Tabla 7. Tipo de impacto o magnitud del daño

| Tipo de Magnitud | | | | |
|------------------|--|---|---|---|
| Nivel | Confidencial, Privado, Sensitivo | Integridad, manipulación, completo | Disponibilidad | Costo de recuperación |
| 4 | El conocimiento o acceso por terceros sin autorización puede conllevar un impacto negativo severo de índole legal, operativa, de pérdida de imagen o económica de la entidad. | Pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad. | Las actividades pueden aplazarse por un máximo de 48 horas. | Los costos de recuperación en (tiempo, económico, material, imagen, emocional) son altos. |
| 3 | El conocimiento o acceso por terceros sin autorización puede conllevar un impacto negativo moderado de índole legal, operativa, de pérdida de imagen o económica a uno o más funcionarios. | Cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad. | Las actividades pueden aplazarse por un máximo de 24 horas. | Los costos de recuperación en (tiempo, económico, material, imagen, emocional) son medios. |
| 2 | Revelación por terceros sin autorización puede conllevar un impacto no significativo. | Cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos. | Las actividades pueden aplazarse por un máximo de 12 horas. | Los costos de recuperación en (tiempo, económico, material, imagen, emocional) son bajos. |
| 1 | Revelación por terceros no conlleva ningún impacto para la entidad o entes externos | Cuya pérdida de exactitud y completitud no conlleva ningún impacto para la entidad o entes externos. | Las actividades pueden aplazarse por un máximo de 6 horas. | Los costos de recuperación en (tiempo, económico, material, imagen, emocional) son insignificantes. |

Fuente. Elaboración propia basada en Ministerio de Hacienda y Administraciones Públicas, 2012 y matriz guía.



| | | |
|---|-------------------------------------|--|
|  INSTITUTO DEPARTAMENTAL DE SALUD <small>NORTE DE SANTANDER</small> | DIRECCIONAMIENTO ESTRATEGICO |  Gobernación de Norte de Santander <small>Instituto Departamental de Salud</small> |
| Código: F-DE-PE05-04 Versión: 05 | COMUNICACION INTERNA | Página 52 de 95 |

La suma de los valores de las propiedades de la magnitud refleja el nivel de impacto o magnitud del activo como lo muestra la siguiente tabla.

Tabla 8 Tabla de impacto o magnitud

| Nivel | Descriptor | Descripción |
|-------|----------------|--|
| 4 | Alto | Activos de información en los cuales la magnitud del impacto es mayor o igual a diez (10), con la suma de los valores de todas sus propiedades (confidencialidad, integridad, disponibilidad y costo de recuperación). |
| 3 | medio | Activos de información en los cuales la magnitud del impacto es ocho (8) o nueve (9), con la suma de los valores de todas sus propiedades (confidencialidad, integridad, disponibilidad y costo de recuperación). |
| 2 | bajo | Activos de información en los cuales la magnitud del impacto es seis (6) o siete (7), con la suma de los valores de todas sus propiedades (confidencialidad, integridad, disponibilidad y costo de recuperación). |
| 1 | insignificante | Activos de información en los cuales la magnitud del impacto es menor o igual a cinco (5), con la suma de los valores de todas sus propiedades (confidencialidad, integridad, disponibilidad y costo de recuperación). |



Fuente. Elaboración propia basada en Ministerio de Hacienda y Administraciones Públicas, 2012 y matriz guía.

Tabla 9 Activos de Información Sistemas e Información

| Sistemas e Infraestructura | Clasificación | | | | | Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto] |
|---|----------------------------------|---------------------------|----------------|---|-----------|---|
| | Confidencial, Privado, Sensitivo | Integridad, manipulación, | Disponibilidad | Costo de recuperación (tiempo, económico, material, imagen, | sumatoria | |
| Equipos de la red cableada (router, switch, etc.) | 2 | 1 | 4 | 2 | 9 | 3 |
| Equipos de la red inalámbrica (router) | 2 | 1 | 4 | 2 | 9 | 3 |
| Servidores | 4 | 4 | 4 | 4 | 16 | 4 |
| Estaciones de trabajo | 4 | 3 | 2 | 2 | 11 | 4 |
| UPS (Sistema de Alimentación ininterrumpida) | 1 | 1 | 4 | 3 | 9 | 3 |
| Impresoras | 1 | 1 | 3 | 3 | 8 | 2 |
| Sistema de Videoconferencia | 1 | 1 | 3 | 4 | 9 | 2 |
| IP PBX (Sistema de telefonía IP) | 1 | 1 | 4 | 3 | 9 | 2 |
| Instalaciones físicas | 1 | 3 | 4 | 4 | 12 | 4 |

Fuente. Elaboración propia basada en la matriz análisis de riesgos guía.



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 53 de 95</p> |

4.3 Caracterización de las amenazas

En la Guía de Gestión de Riesgos (2016, pág. 19) “Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas”.



De acuerdo como lo indica Magerit 3.0, las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño. Amenaza Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008]” (Ministerio de Hacienda y Administraciones Públicas, 2012). El instituto departamental identifico los orígenes de las amenazas como lo demuestra la tabla 10.

Tabla 10. Origen de la Amenaza.

| Origen | Amenaza |
|---|---|
| Actos originados por la criminalidad común y motivación política | Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios. |
| Sucesos de origen físico | Se tienen accidentes naturales tales como: (terremotos, inundaciones, sísmico). Los sistemas información pueden llegar hacer víctima pasiva, es importante tenerla en cuenta lo que puede suceder. |
| Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales | Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión. |

Fuente. Elaboración propia basada en la matriz de análisis y (Ministerio de Hacienda y Administraciones Públicas, 2012)



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 54 de 95</p> |

4.4 Valoración de las amenazas

Las amenazas dependiendo del nivel o dimensiones, se puede perjudicar el activo, valorando la influencia en sentido de probabilidad, pueden causar diferentes impactos dependiendo de los activos que se vean involucrados con el daño.

Probabilidad: cuán probable o improbable es que se materialice la amenaza. Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

La probabilidad de que una vulnerabilidad de manera potencial ocurra por una fuente de amenaza puede definirse en niveles tales como: Insuficiente, bajo, medio o alto.

- Insuficiente: Nivel Insuficiente de probabilidad de amenaza en la seguridad de la información, siendo estos inofensivos, al tener controles hará siempre frenar la vulnerabilidad.
- Bajo: Nivel bajo de probabilidad de amenaza en la seguridad de la información, siendo este carente de motivación, al tener los controles listos para impedir elocuentemente que la vulnerabilidad ocurra.
- Medio: Nivel medio de probabilidad de amenaza en la seguridad de la información, motiva y capaz de causar daño. Al realizar controles a tiempo este frenar el éxito de que la vulnerabilidad ocurra.
- Alto: Alto nivel de probabilidad de amenazas en la seguridad de la información para ellos se realiza un estudio de análisis de riesgo con el fin de identificar y mitigar la vulnerabilidad.





| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 55 de 95</p> |

Tabla 11. Tabla de Probabilidad

| Nivel | Descriptor | Frecuencia | Descripción |
|-------|----------------|----------------|---|
| 4 | Alto | muy frecuente | La probabilidad de que suceda a diario |
| 3 | medio | frecuente | La probabilidad de que suceda mensualmente |
| 2 | bajo | normal | La probabilidad de que suceda una vez al año |
| 1 | insignificante | poco frecuente | La probabilidad que suceda 1 o 2 vez a 5 años |

Fuente. Elaboración propia basada en (Ministerio de Hacienda y Administraciones Públicas, 2012)

En el proceso de caracterización de las amenazas de acuerdo a la matriz usada para el análisis del riesgo (Erb, 2015) , se agruparon en tres grandes grupos las cuales son: 1. Actos originados por la criminalidad común y motivación política, 2. Sucesos de origen físico y 3. Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales, los cuales en su interior están compuestos de un gran número de amenazas descritas en las tablas siguientes con su magnitud de daño.

Tabla 12 Amenazas por actos originados por la criminalidad común y motivación política

| Origen | Amenaza | Nivel de Probabilidad | Descriptor |
|---|--|-----------------------|----------------|
| Actos originados por la criminalidad común y motivación política | Sabotaje (ataque físico y electrónico) | 1 | Insignificante |
| | Robo / Hurto (físico) | 2 | Bajo |
| | Robo / Hurto de información electrónica | 2 | Bajo |
| | Intrusión a Red interna | 3 | Medio |
| | Virus / Ejecución no autorizado de programas | 3 | Medio |

Fuente. Elaboración propia tomada de la matriz de análisis (Erb, 2015)





| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 56 de 95</p> |

Tabla 13 Amenazas por sucesos de origen físico

| Origen | Amenaza | Nivel de Probabilidad | Descriptor |
|--------------------------|------------------------------------|-----------------------|----------------|
| Sucesos de origen físico | Incendio | 1 | Insignificante |
| | Inundación / deslave | 1 | Insignificante |
| | Sismo | 4 | Alto |
| | Falla de corriente (apagones) | 3 | Medio |
| | Falla de sistema / Daño disco duro | 4 | Alto |

Fuente. Elaboración propia tomada de la matriz de análisis (Erb, 2015)

Tabla 14 Amenaza por sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales.

| Origen | Amenaza | Nivel de Probabilidad | Descriptor |
|--|--|-----------------------|------------|
| Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales | Falta de inducción, capacitación y sensibilización sobre riesgos | 4 | Alto |
| | Utilización de programas no autorizados / software 'pirateado' | 2 | Bajo |
| | Falta de pruebas de software nuevo con datos productivos | 3 | Medio |
| | Infección de sistemas a través de unidades portables sin escaneo | 4 | Alto |
| | Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada) | 3 | Medio |
| | Falta de actualización de software (proceso y recursos) | 4 | Alto |

Fuente. Elaboración propia tomada de la matriz de análisis (Erb, 2015)



4.5 Estimación del estado del riesgo

La estimación del estado del riesgo tiene como fin valorar su grado de riesgo; determinando los componentes que requieren protección, las vulnerabilidades que lo debilitan y las amenazas que lo pueden afectar (Erb, 2015).

El riesgo se calcula de acuerdo a la siguiente fórmula:

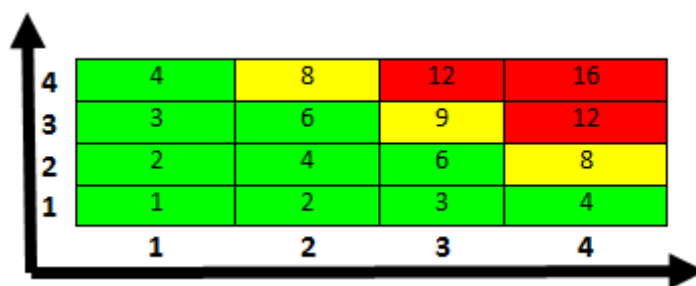
$$\text{Riesgo} = \text{probabilidad de amenazas} * \text{magnitud de daño}$$



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 57 de 95</p> |

Y para su identificación se estableció los colores: verde para bajo, amarillo para medio y rojo para alto en donde, que representa la recopilación y promedio de la valoración por cada ítem.

Ilustración 4. Valoración del riesgo



Fuente. Basado en Matriz para el análisis de riesgos (Erb, 2015)

Ilustración 5. Rango de Riesgo



Fuente. Elaboración propia basado en Matriz para el análisis de riesgos (Erb, 2015)

Para realizar la gestión del riesgo se tiene cuatro opciones de manejo las cuales están definidas y descritas en la siguiente tabla:

Tabla 15. Opciones de manejo de los riesgos

| Opciones de manejo | Descripción |
|--|---|
| Evitar el riesgos | Se evitan todos los riesgos a los cuales se le puede eliminar la causa raíz del riesgo y que el rango sea ALTO o MEDIO. |
| Reducir el riesgos | Se reducen todos los riesgos que se puede disminuir la frecuencia del mismo o su materialización futura en el rango ALTO o MEDIO. |
| Compartir o transferir el riesgos | Se comparten los riesgos cuando otra proceso o entidad puede asumir acciones que disminuyan la frecuencia del mismo o su materialización futura el riesgo y que el rango sea ALTO |
| Aceptar el riesgos | Se asumen los riesgos que el costo de la mitigación es mayor al impacto que causará al materializarse el riesgo y que el rango sea BAJO. |

Fuente. Elaboración propia



Resultados de valoración de Magnitud del daño con las amenazas.

Ilustración 6. Valoración de Datos e información de acuerdo a las amenazas originadas por la criminalidad.

| Datos e Información | Clasificación | | | | | sumatoria | Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto] | Actos originados por la criminalidad | | | | |
|--|----------------------------------|------------------------------------|----------------|--------------------------------|----|-----------|--|--|-----------------------|-----------------------------|-------------------------|------------------------------------|
| | Confidencial, Privado, Sensitivo | Integridad, manipulación, completo | Disponibilidad | Costo de recuperación (tiempo, | | | | Sabotaje (ataque físico y electrónico) | Robo / Hurto (físico) | Robo / Hurto de información | Intrusión a Red interna | Virus / Ejecución no autorizado de |
| | | | | | | | | 1 | 2 | 2 | 3 | 3 |
| Documentos institucionales (Planes, Informes, Seguimientos, Contratación etc.) | 4 | 3 | 1 | 1 | 9 | 3 | 3 | 6 | 6 | 9 | 9 | 9 |
| Portales Bancarios | 4 | 4 | 4 | 1 | 13 | 4 | 4 | 8 | 8 | 12 | 12 | 12 |
| Correo electrónico | 4 | 4 | 4 | 3 | 15 | 4 | 4 | 8 | 8 | 12 | 12 | 12 |
| Bases de datos institucionales | 4 | 3 | 3 | 3 | 13 | 4 | 4 | 8 | 8 | 12 | 12 | 12 |
| Almacenamiento de información(organización de la información y buenas practicas) | 3 | 4 | 3 | 3 | 13 | 3 | 3 | 6 | 6 | 9 | 9 | 9 |
| Firma Digital | 4 | 4 | 4 | 2 | 14 | 4 | 4 | 8 | 8 | 12 | 12 | 12 |
| Página Web Institucional | 2 | 4 | 4 | 4 | 14 | 4 | 4 | 8 | 8 | 12 | 12 | 12 |
| Telefonía IP | 1 | 3 | 2 | 3 | 9 | 3 | 3 | 6 | 6 | 9 | 9 | 9 |

Fuente. Elaboración propia basa en matriz guía.

Ilustración 7. Valoración de Datos e información de acuerdo a las amenazas originadas por sucesos de origen físico.

| Datos e Información | Clasificación | | | | | sumatoria | Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto] | Sucesos de origen físico | | | | |
|--|----------------------------------|------------------------------------|----------------|--------------------------------|----|-----------|--|--------------------------|----------------------|-------|-------------------------------|-------------------------------|
| | Confidencial, Privado, Sensitivo | Integridad, manipulación, completo | Disponibilidad | Costo de recuperación (tiempo, | | | | Incendio | Inundación / deslave | Sismo | Falla de corriente (apagones) | Falla de sistema / Daño disco |
| | | | | | | | | 1 | 1 | 4 | 3 | 4 |
| Documentos institucionales (Planes, Informes, Seguimientos, Contratación etc.) | 4 | 3 | 1 | 1 | 9 | 3 | 3 | 3 | 12 | 9 | 12 | 12 |
| Portales Bancarios | 4 | 4 | 4 | 1 | 13 | 4 | 4 | 4 | 16 | 12 | 16 | 16 |
| Correo electrónico | 4 | 4 | 4 | 3 | 15 | 4 | 4 | 4 | 16 | 12 | 16 | 16 |
| Bases de datos institucionales | 4 | 3 | 3 | 3 | 13 | 4 | 4 | 4 | 16 | 12 | 16 | 16 |
| Almacenamiento de información(organización de la información y buenas practicas) | 3 | 4 | 3 | 3 | 13 | 3 | 3 | 3 | 12 | 9 | 12 | 12 |
| Firma Digital | 4 | 4 | 4 | 2 | 14 | 4 | 4 | 4 | 16 | 12 | 16 | 16 |
| Página Web Institucional | 2 | 4 | 4 | 4 | 14 | 4 | 4 | 4 | 16 | 12 | 16 | 16 |
| Telefonía IP | 1 | 3 | 2 | 3 | 9 | 3 | 3 | 3 | 12 | 9 | 12 | 12 |

Fuente. Elaboración propia basa en matriz guía.



Ilustración 8. Valoración de Datos e información de acuerdo a las amenazas originadas por Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales.

| Datos e Información | Clasificación | | | | | sumatoria | Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto] | Sucesos derivados de la impericia, ne | | | | |
|--|----------------------------------|------------------------------------|----------------|--------------------------------|----------------------------------|-----------|--|---|----------------------|------------------------------------|----|---|
| | Confidencial, Privado, Sensitivo | Integridad, manipulación, completo | Disponibilidad | Costo de recuperación (tiempo) | Falta de inducción, capacitación | | | Utilización de programas no autorizados / infección de sistemas a través de | Manejo inadecuado de | Falta de actualización de software | | |
| | | | | | | | | | | | 4 | 2 |
| Documentos institucionales (Planes, Informes, Seguimientos, Contratación etc.) | 4 | 3 | 1 | 1 | 9 | 3 | 12 | 6 | 12 | 9 | 9 | |
| Portales Bancarios | 4 | 4 | 4 | 1 | 13 | 4 | 16 | 8 | 16 | 12 | 12 | |
| Correo electrónico | 4 | 4 | 4 | 3 | 15 | 4 | 16 | 8 | 16 | 12 | 12 | |
| Bases de datos institucionales | 4 | 3 | 3 | 3 | 13 | 4 | 16 | 8 | 16 | 12 | 12 | |
| Almacenamiento de información(organización de la información y buenas practicas) | 3 | 4 | 3 | 3 | 13 | 3 | 12 | 6 | 12 | 9 | 9 | |
| Firma Digital | 4 | 4 | 4 | 2 | 14 | 4 | 16 | 8 | 16 | 12 | 12 | |
| Página Web Institucional | 2 | 4 | 4 | 4 | 14 | 4 | 16 | 8 | 16 | 12 | 12 | |
| Telefonía IP | 1 | 3 | 2 | 3 | 9 | 3 | 12 | 6 | 12 | 9 | 9 | |

Fuente. Elaboración propia basa en matriz guía.

Ilustración 9. Valoración de Sistemas e Infraestructura de acuerdo a las amenazas originadas por la criminalidad.

| Sistemas e Infraestructura | Clasificación | | | | | sumatoria | Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto] | Sabotaje (ataque físico y electrónico) | Robo / Hurto (físico) | Robo / Hurto de | Intrusión a Red interna | Virus / Ejecución no autorizado de programas | | | |
|---|----------------------------------|------------------------------------|----------------|---|----------------------------------|-----------|--|--|-----------------------|-----------------|-------------------------|--|---|----------------------|------------------------------------|
| | Confidencial, Privado, Sensitivo | Integridad, manipulación, completo | Disponibilidad | Costo de recuperación (tiempo, económico, material, imagen, | Falta de inducción, capacitación | | | | | | | | Utilización de programas no autorizados / infección de sistemas a través de | Manejo inadecuado de | Falta de actualización de software |
| | | | | | | | | | | | | | | | |
| Equipos de la red cableada (router, switch, etc.) | 2 | 1 | 4 | 2 | 9 | 3 | 3 | 6 | 6 | 9 | 9 | | | | |
| Equipos de la red inalámbrica (router) | 2 | 1 | 4 | 2 | 9 | 3 | 3 | 6 | 6 | 9 | 9 | | | | |
| Servidores | 4 | 4 | 4 | 4 | 16 | 4 | 4 | 8 | 8 | 12 | 12 | | | | |
| Estaciones de trabajo | 4 | 3 | 2 | 2 | 11 | 4 | 4 | 8 | 8 | 12 | 12 | | | | |
| UPS (Sistema de Alimentación ininterrumpida) | 1 | 1 | 4 | 3 | 9 | 3 | 3 | 6 | 6 | 9 | 9 | | | | |
| Impresoras | 1 | 1 | 3 | 3 | 8 | 2 | 2 | 4 | 4 | 6 | 6 | | | | |
| Sistema de Videoconferencia | 1 | 1 | 3 | 4 | 9 | 2 | 2 | 4 | 4 | 6 | 6 | | | | |
| IP PBX (Sistema de telefonía IP) | 1 | 1 | 4 | 3 | 9 | 2 | 2 | 4 | 4 | 6 | 6 | | | | |
| Instalaciones físicas | 1 | 3 | 4 | 4 | 12 | 4 | 4 | 8 | 8 | 12 | 12 | | | | |

Fuente. Elaboración propia basa en matriz guía.



Ilustración 10. Valoración de Sistemas e Infraestructura de acuerdo a las amenazas originadas por sucesos de origen físico.

| Sistemas e Infraestructura | Clasificación | | | | | Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto] | Sucesos de origen físico | | | | |
|---|----------------------------------|------------------------------------|----------------|--|----|--|--------------------------|----------------------|-------|-------------------------------|------------------------------------|
| | Confidencial, Privado, Sensitivo | Integridad, manipulación, completo | Disponibilidad | Costo de recuperación (tiempo, económico, material, imagen, sumatoria) | | | Incendio | Inundación / deslave | Sismo | Falla de corriente (apagones) | Falla de sistema / Daño disco duro |
| Equipos de la red cableada (router, switch, etc.) | 2 | 1 | 4 | 2 | 9 | 3 | 3 | 3 | 12 | 9 | 12 |
| Equipos de la red inalámbrica (router) | 2 | 1 | 4 | 2 | 9 | 3 | 3 | 3 | 12 | 9 | 12 |
| Servidores | 4 | 4 | 4 | 4 | 16 | 4 | 4 | 4 | 16 | 12 | 16 |
| Estaciones de trabajo | 4 | 3 | 2 | 2 | 11 | 4 | 4 | 4 | 16 | 12 | 16 |
| UPS (Sistema de Alimentación ininterrumpida) | 1 | 1 | 4 | 3 | 9 | 3 | 3 | 3 | 12 | 9 | 12 |
| Impresoras | 1 | 1 | 3 | 3 | 8 | 2 | 2 | 2 | 8 | 6 | 8 |
| Sistema de Videoconferencia | 1 | 1 | 3 | 4 | 9 | 2 | 2 | 2 | 8 | 6 | 8 |
| IP PBX (Sistema de telefonía IP) | 1 | 1 | 4 | 3 | 9 | 2 | 2 | 2 | 8 | 6 | 8 |
| Instalaciones físicas | 1 | 3 | 4 | 4 | 12 | 4 | 4 | 4 | 16 | 12 | 16 |



Fuente. Elaboración propia basa en matriz guía.

Ilustración 11. Valoración de Sistemas e Infraestructura de acuerdo a las amenazas originadas por Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales.

| Sistemas e Infraestructura | Clasificación | | | | | Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto] | Sucesos derivados de impericia, negligencia de usuarios/as y decisiones institucionales | | | | |
|--|----------------------------------|------------------------------------|----------------|--|----|--|---|--|--|--|--|
| | Confidencial, Privado, Sensitivo | Integridad, manipulación, completo | Disponibilidad | Costo de recuperación (tiempo, económico, material, imagen, sumatoria) | | | Falta de inducción, capacitación y sensibilización sobre | Utilización de programas no autorizados / software | Infección de sistemas a través de unidades portables sin escaneo | Manejo inadecuado de contraseñas (inseguras, no) | Falta de actualización de software (procesos y recursos) |
| Equipos de la red cableada | 2 | 1 | 4 | 2 | 9 | 3 | 4 | 2 | 6 | 12 | 9 |
| Equipos de la red inalámbrica | 2 | 1 | 4 | 2 | 9 | 3 | 4 | 2 | 6 | 12 | 9 |
| Servidores | 4 | 4 | 4 | 4 | 16 | 4 | 4 | 4 | 16 | 12 | 16 |
| Estaciones de trabajo | 4 | 3 | 2 | 2 | 11 | 4 | 4 | 4 | 16 | 12 | 16 |
| UPS (Sistema de Alimentación ininterrumpida) | 1 | 1 | 4 | 3 | 9 | 3 | 4 | 2 | 6 | 12 | 9 |
| Impresoras | 1 | 1 | 3 | 3 | 8 | 2 | 4 | 2 | 8 | 6 | 8 |
| Sistema de Videoconferencia | 1 | 1 | 3 | 4 | 9 | 2 | 4 | 2 | 8 | 6 | 8 |
| IP PBX (Sistema de telefonía IP) | 1 | 1 | 4 | 3 | 9 | 2 | 4 | 2 | 8 | 6 | 8 |
| Instalaciones físicas | 1 | 3 | 4 | 4 | 12 | 4 | 4 | 4 | 16 | 12 | 16 |

Fuente. Elaboración propia basa en matriz guía.



| | | |
|---|-------------------------------------|--|
|  INSTITUTO DEPARTAMENTAL DE SALUD <small>NORTE DE SANTANDER</small> | DIRECCIONAMIENTO ESTRATEGICO |  Gobernación de Norte de Santander <small>Instituto Departamental de Salud</small> |
| Código: F-DE-PE05-04 Versión: 05 | COMUNICACION INTERNA | Página 61 de 95 |

4.6 Análisis de Resultado de la Valoración y Definición de los Riesgos.

En las tablas 20 y 21 se describen los riesgos con la valoración MEDIO y ALTO, a los cuales se establecerán las opciones de manejo a aplicar, en cuanto a los riesgos de valoración BAJO la empresa los acepta.

Tabla 16 Resultado del análisis de riesgo con evaluación Medio

| RIESGO | TIPO DE RIESGO | CALIFICACION MAGNITUD*PROBABILIDAD | TIPO DE IMPACTO | EVALUCION RIESGO | OPCIONES DE MANEJO |
|--|--------------------|------------------------------------|----------------------------|------------------|--------------------|
| R1: Falla de Seguridad incluye robo, hurto, Intrusión Afectación por Virus o Ejecución no autorizado de programas: | Riesgos operativos | 9 | Disponibilidad/ integridad | MEDIO | Reducir el riesgos |
| R1a: a documentos, medios de almacenamiento o telefonía. | Riesgos operativos | 9 | Integridad | MEDIO | Reducir el riesgos |
| R1b: a dispositivos de la red. | Riesgos operativos | 9 | Disponibilidad | MEDIO | Reducir el riesgos |
| R1c: a medios de almacenamiento. | Riesgos operativos | 9 | Integridad | MEDIO | Reducir el riesgos |
| R1d: a telefonía IP. | Riesgos operativos | 9 | Disponibilidad | MEDIO | Reducir el riesgos |
| R2: Perdida de información: | Riesgos operativos | 9 | Confidencialidad | MEDIO | Reducir el riesgos |
| R2a: por manejo inadecuado de contraseñas. | Riesgos operativos | 9 | Confidencialidad | MEDIO | Reducir el riesgos |
| R2b: por uso de software no legal. | Riesgos operativos | 9 | Confidencialidad | MEDIO | Reducir el riesgos |

Fuente. Elaboración propia.







| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 62 de 95</p> |

Tabla 17 Resultado de análisis de riesgo con evaluación Alto

| RIESGO | TIPO DE RIESGO | CALIFICACION MAGNITUD*PROBABILIDAD | TIPO DE IMPACTO | EVALUACION RIESGO | OPCIONES DE MANEJO |
|---|----------------------|------------------------------------|---|-------------------|--------------------|
| R3: Falla de Seguridad incluye robo, hurto, Intrusión Afectación por Virus o Ejecución no autorizado de programas: | Riesgos tecnológicos | 12 | Disponibilidad / costos de reproducción | ALTO | Evitar el riesgos |
| R3a: a portales web | Riesgos tecnológicos | 12 | Disponibilidad | ALTO | Evitar el riesgos |
| R3b: a firma digital. | Riesgos tecnológicos | 12 | Disponibilidad | ALTO | Evitar el riesgos |
| R3c: a servidores y estaciones de trabajo. | Riesgos tecnológicos | 12 | Costos de reproducción | ALTO | Evitar el riesgos |
| R4: Perdida de información incluye falla sísmica, falla de sistema / Daño disco duro o desconocimiento y falta de capacitación de los usuarios: | Riesgos operativos | 16 | Integridad | ALTO | Evitar el riesgos |
| R4a: a dispositivos de la red. | Riesgos operativos | 12 | Costos de reproducción | ALTO | Evitar el riesgos |
| R4b: a servidores y estaciones de trabajo. | Riesgos operativos | 16 | Costos de reproducción | ALTO | Evitar el riesgos |
| R5: Desconocer los riesgos de afectar: | Riesgos operativos | 16 | Disponibilidad | ALTO | Evitar el riesgos |
| R5a: los servidores. | Riesgos tecnológicos | 16 | Costos de reproducción | ALTO | Evitar el riesgos |
| R5b: estaciones de trabajo. | Riesgos tecnológicos | 12 | Costos de reproducción | ALTO | Evitar el riesgos |

Fuente. Elaboración propia

| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 63 de 95</p> |

5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN



La finalidad de un Sistema de Gestión de Seguridad de la Información es garantizar la continuidad del negocio, es decir, proporcionar una herramienta de gestión integral y continuo que aporte a la sostenibilidad de la organización en pro del logro tanto de la misión como la visión.

El Sistema de Gestión de Seguridad de la Información nos permite minimizar los riesgos, ya que se identifican y gestionan por la organización de manera documentada y estructurada; de forma que se pueda establecer un plan estratégico que mitigue las consecuencias de éstos y que no se vea afectado la operación diaria de la organización, pero que a la vez aporte a la Estrategia Organizacional, así como lo expresan Bueno, Correa, & Echeverry (2010) que fomente la innovación mejorando los resultados, los costos y los riesgos, logrando el funcionamiento óptimo de la empresa. Al presentarse como un sistema continuo y proactivo aporta al conocimiento propio de la organización en todos los niveles y a la vez, puede proporcionar acciones de mejora para el negocio aportando de ésta manera a la sostenibilidad y con un enfoque diferenciador.

5.1 Controles del Sistema de gestión de Seguridad de la Información

En este apartado se identifican controles que ayudan a evitar trabajo o costos innecesarios, además se verifican los controles existentes para validar si funcionan correctamente.





| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 64 de 95</p> |

(Ministerio de Hacienda y Administraciones Públicas, 2012) Definen los controles o las salvaguardas “como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo”, y describe los tipos de controles que existen como lo son:

- **Controles preventivos (CP):** Son los controles que reducen las oportunidades de que un incidente ocurra. Si el control falla y el incidente llega a ocurrir, los daños son los mismos. Ejemplos: autorización previa de los usuarios gestión de privilegios.
- **Controles detectivos (CD):** Son controles que su función es detectar un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sí permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños. Ejemplos: anti-virus.
- **Controles correctivos (CC):** Son controles que actúan después de que el incidente se haya producido y por tanto reducen los daños. Ejemplos: gestión de incidentes, líneas de comunicación alternativas, fuentes de alimentación redundantes.
- **Controles de recuperación (CR):** Son controles que permite regresar al estado anterior al incidente. Son controles que no reducen las probabilidades del incidente, pero acotan los daños a un periodo de tiempo. Ejemplos: copias de seguridad (back-up).
- **Controles disuasivos (CS):** Son controles que generan un efecto tal sobre los atacantes que estos no se atreven o se lo piensan dos veces antes de atacar. Son controles que actúan antes del incidente, reduciendo las probabilidades de que ocurra; pero que no tienen influencia sobre los daños causados caso de que el atacante realmente se atreva. Ejemplos: vallas elevadas, guardias de seguridad, avisos sobre la persecución del delito o persecución del delincuente



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 65 de 95</p> |

- A continuación se relacionan los controles establecidos para el Sistema de Gestión de Seguridad de la Información basados en los Controles de Seguridad y Privacidad de la Información (MinTIC, 2016) que menciona los controles del Anexo A de la norma NTC: ISO/IEC 27001 (ICONTEC, 2006):

Tabla 18 Definición de Controles para el SGSI

| Identificación del Control | Homologación | Tipo de Control | Nombre | Descripción |
|----------------------------|--------------|-----------------|---|--|
| CT01 | A.5 | | Políticas de seguridad de la información | |
| CT01.1 | A.5.1 | | Directrices establecidas por la dirección para la seguridad de la información | Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes. |
| CT01.1.1 | A.5.1.1 | CP | Políticas para la seguridad de la información. | Control: Se encuentran definidas las políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes |
| CT01.1.2 | A.5.1.2 | CP | Revisión de las políticas para seguridad de la información | Control: Las políticas para seguridad de la información se revisan a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia Continuas |
| CT02 | A.9 | | Control de Acceso | |
| CT02.1 | A.9.1 | | Requisitos del negocio para control de acceso | Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información. |
| CT02.1.1 | A.9.1.1 | CP | Política de control de acceso | Control: Se establece, documenta y revisa la política de control de acceso con base en los requisitos del negocio y de seguridad de la información. |
| CT02.1.2 | A.9.1.2 | CP | Política sobre el uso de los servicios de red | Control: Solo se permite acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente. |
| CT02.2 | A.9.4 | | Control de acceso a sistemas y aplicaciones | Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones. |
| CT02.2.1 | A.9.4.3 | CD | Sistema de gestión de contraseñas | Control: Los sistemas de gestión de contraseñas son interactivos y se asegura la calidad de las contraseñas. |

Fuente. Elaboración propia







| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 66 de 95</p> |

Tabla 19. Definición de Controles para el SGSI (Continuación)

| Identificación del Control | Homologación | Tipo de Control | Nombre | Descripción |
|----------------------------|--------------|-----------------|---|--|
| CT03 | A.11 | | Seguridad física y del entorno | |
| CT03.1 | A.11.2 | | Equipos | Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. |
| CT03.1.1 | A.11.2.1 | CD | Ubicación y protección de los equipos | Control: Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado. |
| CT03.1.2 | A.11.2.2 | CC | Servicios de suministro | Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. |
| CT03.1.3 | A.11.2.4 | CP | Mantenimiento de equipos | Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas. |
| CT03.1.4 | A.11.2.5 | CS | Retiro de activos | Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa. |
| CT03.1.5 | A.11.2.9 | CP | Política de escritorio limpio y pantalla limpia | Control: Adopción de una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información. |
| CT04 | A.12 | | Seguridad de las operaciones | |
| CT04.1 | A.12.3 | | Copias de respaldo | Objetivo: Proteger contra la pérdida de datos. |
| CT04.1.1 | A.12.3.1 | CR | Respaldo de información | Control: Se deben hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una Política de copias de respaldo aceptada. |
| CT04.2 | A.12.6 | | Gestión de la vulnerabilidad técnica | Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas. |
| CT04.2.1 | A.12.6.2 | CP | Restricciones sobre la instalación de software | Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios. |

Fuente. Elaboración propia



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 67 de 95</p> |

5.2 Indicadores Propuestos para el Sistema de Gestión de Seguridad de la Información.

De acuerdo a la Guía de indicadores de gestión para la seguridad de la información (MinTIC, 2015) los indicadores permite medir la efectividad, eficiencia y eficacia de lo establecido, los cuales, servirán como insumo para la mejora continua permitiendo adoptar decisiones que apoye el mejoramiento de la organización.

Se pueden establecer indicadores:

- Estratégicos que se encuentran vinculados a la estrategia organizacional
- Tácticos que se relaciona a los procesos
- Operativos que se encuentra vinculados a la gestión y cumplimiento de las actividades de los procesos.

Para el proceso seleccionado PLANEACIÓN ESTRATÉGICA, en donde se encuentra las TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES que se encuentra inmerso dentro del macro proceso DIRECCIONAMIENTO ESTRATÉGICO del Instituto Departamental de Salud de Norte de Santander se estableció indicador táctico e indicadores operativos para medir la gestión del proceso y el cumplimiento de las tareas asignadas. En él se encuentra la definición de cada uno de los indicadores. A continuación se relaciona los indicadores definidos para los controles establecidos.





| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 68 de 95</p> |

Tabla 20 Relación de Indicadores por Controles

| Tipo de Indicador | Identificación del Indicador | Nombre del Indicador | Nombre del Control |
|-------------------|------------------------------|--|--|
| Táctico | Indicador01 | Implementación de las políticas de seguridad de la información | Políticas para la seguridad de la información. |
| Táctico | Indicador02 | Cobertura de la política | Revisión de las políticas para seguridad de la información |
| Operativo | Indicador03 | Establecimiento de control de acceso | Política de control de acceso |
| Operativo | Indicador04 | Acceso controlado a los servicios de red | Política sobre el uso de los servicios de red |
| Operativo | Indicador05 | Contraseñas establecidas | Sistema de gestión de contraseñas |
| Operativo | Indicador06 | Implementación de antivirus | Ubicación y protección de los equipos |
| Operativo | Indicador07 | Respaldo de suministro de energía a los equipos de red | Servicios de suministro |
| Operativo | Indicador08 | Seguimiento de solicitudes | Mantenimiento de equipos |
| Operativo | Indicador09 | Grado de retiro de activos no autorizados | Retiro de activos |
| Operativo | Indicador10 | Formación en buenas practicas | Política de escritorio limpio y pantalla limpia |
| Operativo | Indicador11 | Implementación de política de almacenamiento de información | Respaldo de información |
| Operativo | Indicador12 | Restricciones establecidas | Restricciones sobre la instalación de software |

Fuente. Elaboración propia.

5.3. Valoración de acuerdo a los controles

A continuación se relaciona la escala de valoración acuerdo a dos parámetros las herramientas para ejercer el control y el seguimiento al control.





| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 69 de 95</p> |

Tabla 21 Parámetros de valoración para los Controles

| PARAMETROS DE VALORACION | CRITERIOS | PUNTAJE |
|--------------------------------------|---|---------|
| Herramientas para ejercer el control | No existe | 0 |
| | Posee una herramienta para ejercer el control. | 15 |
| | Posee una herramienta para ejercer control con manuales instructivos o procedimientos | 30 |
| | Se ha demostrado en el tiempo que lleva la herramienta ser efectiva | 60 |
| seguimiento al control | No existe | 0 |
| | Están definidos los responsables de la ejecución del control y del seguimiento | 15 |
| | La frecuencia de la ejecución del control y seguimiento es adecuada | 40 |

Fuente. Elaboración propia basado en la Guía para la Administración del Riesgo (DAFP, 2011)

El puntaje final corresponderá a la sumatoria de los dos criterios.



Una vez valorado se obtiene el riesgo residual, en donde se especifica la nueva valoración y el tratamiento que se le debe dar al riesgo. A continuación se visualiza los posibles rangos de calificación de acuerdo al puntaje final:

Tabla 22 Rango de calificación de los controles

| RANGOS DE CALIFICACIÓN DE LOS CONTROLES | CANTIDAD A DISMINUIR EN EL RANGO DE RIESGO |
|---|--|
| Entre 0-50 | 0 |
| Entre 51-75 | 1 |
| Entre 76-100 | 2 |

Fuente. Elaboración propia basado en la Guía para la Administración del Riesgo (DAFP, 2011)



| | | |
|---|-------------------------------------|--|
|  INSTITUTO DEPARTAMENTAL DE SALUD <small>NORTE DE SANTANDER</small> | DIRECCIONAMIENTO ESTRATEGICO |  Gobernación de Norte de Santander <small>Instituto Departamental de Salud</small> |
| Código: F-DE-PE05-04 Versión: 05 | COMUNICACION INTERNA | Página 70 de 95 |

5.3.1. Resultados de la Valoración

Ilustración 12 Valoración del Riesgo

| RIE SGO | EVALUCION RIESGO | Controles | | | | |
|--|------------------|-----------------|---|---|--|---|
| | | Tipo de control | Control | Responsable | Documento | Evidencia |
| R1: Falla de Seguridad incluye robo, hurto, Intrusión Afectación por Virus o Ejecución no autorizado de programas: | MEDIO | CP | CT01.1.1 Políticas para la seguridad de la información | Comité Antitrámites y GD | Política de Seguridad de Información | Publicación en la página web |
| | MEDIO | CP | CT01.1.2 Revisión de las políticas para seguridad de la información | Control Interno y Sistemas de información | Auditorías Actas de Reunión | Formatos de auditorías y actas de reunión diligenciados |
| R1a: a documentos | MEDIO | CR | CT04.1.1 Respaldo de información | Sistemas de Información | Política específica de respaldo de información | Publicación en la página web |
| | MEDIO | CD | CT03.1.1 Ubicación y protección de los equipos | Sistemas de Información | * Hoja de vida de los equipos de cómputo y comunicaciones * Revisiones periódicas | * Formatos diligenciados * Actas de revisiones |
| R1b: a dispositivos de la red. | MEDIO | CP | CT02.1.2 Política sobre el uso de los servicios de red | Sistemas de Información | * Política de Acceso * Auditorías de seguimiento | * Publicación página web * Actas de auditorías de seguimiento * Solicitudes de Servicio técnico |
| R1c: a medios de almacenamiento. | MEDIO | CR | CT04.1.1 Respaldo de información | Sistemas de Información | Política específica de respaldo de información | Publicación en la página web |
| R1d: a telefonía IP. | MEDIO | CP | CT01.1.1 Políticas para la seguridad de la información | Comité Antitrámites y GD | Política de Seguridad de Información | Publicación en la página web |
| | MEDIO | CD | CT03.1.1 Ubicación y protección de los equipos | Sistemas de Información | * Hoja de vida de los equipos de cómputo y comunicaciones * Revisiones periódicas | * Formatos diligenciados * Actas de revisiones |
| R2: Perdida de información: | MEDIO | CR | CT04.1.1 Respaldo de información | Sistemas de Información | Política específica de respaldo de información | Publicación en la página web |
| R2a: por manejo inadecuado de contraseñas. | MEDIO | CD | CT02.2.1 Sistema de gestión de contraseñas | Planeación y Sistemas de Información | Política de Seguridad de Información | Publicación en la página web |
| R2b: por uso de software no legal. | MEDIO | CP | CT04.2.1 Restricciones sobre la instalación de software | Sistemas de Información | Política de Seguridad de Información | Publicación en la página web |

Fuente. Elaboración propia.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 71 de 95</p> |

Ilustración 13 Valoración del Riesgo (Continuación)

| RIESGO | VALORACIÓN | | | | | DISMINUIR | | RIESGO RESIDUAL | |
|--|---|---|--|--|---------------|------------------------------------|---------------------------------|--------------------|----------------------|
| | HERRAMIENTA PARA EJERCER EL CONTROL | PUNTAJE HERRAMIENTA PARA EJERCER EL CONTROL | HERRAMIENTA SEGUIMIENTO AL CONTROL | PUNTAJE HERRAMIENTA SEGUIMIENTO AL CONTROL | PUNTAJE FINAL | Rango de Calificación de Controles | CANTIDAD DE NIVELES A DISMINUIR | NUEVA CALIFICACION | MEDIDAS DE RESPUESTA |
| R1: Falla de Seguridad incluye robo, hurto, Intrusión Afectación por Virus o Ejecución no autorizado de programas: | Posee una herramienta para ejercer el control. | 15 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 30 | Entre 0-50 | 0 | MEDIO | EVITAR EL RIESGOS |
| | Se ha demostrado en el tiempo que lleva la herramienta ser efectiva | 60 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 75 | Entre 51-75 | 1 | BAJO | ACEPTAR EL RIESGO |
| R1a: a documentos | Posee una herramienta para ejercer el control. | 15 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 30 | Entre 0-50 | 0 | MEDIO | EVITAR EL RIESGOS |
| | Posee una herramienta para ejercer control con manuales instructivos o procedimientos | 30 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 45 | Entre 0-50 | 0 | MEDIO | REDUCIREL RIESGOS |
| R1b: a dispositivos de la red. | Posee una herramienta para ejercer control con manuales instructivos o procedimientos | 30 | La frecuencia de la ejecución del control y seguimiento es adecuada | 40 | 70 | Entre 51-75 | 1 | BAJO | ACEPTAR EL RIESGO |
| R1c: a medios de almacenamiento. | Posee una herramienta para ejercer el control. | 15 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 30 | Entre 0-50 | 0 | MEDIO | EVITAR EL RIESGOS |
| R1d: a telefonía IP. | Posee una herramienta para ejercer el control. | 15 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 30 | Entre 0-50 | 0 | MEDIO | EVITAR EL RIESGOS |
| | Posee una herramienta para ejercer control con manuales instructivos o procedimientos | 30 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 45 | Entre 0-50 | 0 | MEDIO | REDUCIREL RIESGOS |
| R2: Pérdida de información: | Posee una herramienta para ejercer el control. | 15 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 30 | Entre 0-50 | 0 | MEDIO | EVITAR EL RIESGOS |
| R2a: por manejo inadecuado de contraseñas. | Posee una herramienta para ejercer el control | 15 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 30 | Entre 0-50 | 0 | MEDIO | EVITAR EL RIESGOS |
| R2b: por uso de software no legal. | Posee una herramienta para ejercer el control. | 15 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 30 | Entre 0-50 | 0 | MEDIO | REDUCIREL RIESGOS |

Fuente. Elaboración propia.



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 72 de 95</p> |

Ilustración 14 Valoración del Riesgo (Continuación)

| RIESGO | EVALUACION RIESGO | CONTROLES | | | | |
|---|-------------------|-----------------|---|---|---|---|
| | | Tipo de control | Control | Responsable | Documento | Evidencia |
| R3: Falla de Seguridad incluye robo, hurto, Intrusión Afectación por Virus o Ejecución no autorizado de programas: | ALTO | CP | CT01.1.1 Políticas para la seguridad de la información | Comité Antitrámites y GD | Política de Seguridad de Información | Publicación en la página web |
| | ALTO | CP | CT01.1.2 Revisión de las políticas para seguridad de la información | Control Interno y Sistemas de Información | Auditorías Actas de Reunión con los funcionarios | Formatos de auditorías y actas de reunión diligenciados |
| | ALTO | CP | CT02.1.1 Política de control de acceso | Sistemas de Información | * Política Específica de Control de Acceso * Auditorías de seguimiento | * Publicación página web * Actas de auditorías de seguimiento * Solicitudes de Servicio técnico |
| R3a: a portales web | ALTO | CP | CT02.1.1 Política de control de acceso | Sistemas de Información | * Política Específica de Control de Acceso * Auditorías de seguimiento | * Publicación página web * Actas de auditorías de seguimiento * Solicitudes de Servicio técnico |
| R3b: a firma digital. | ALTO | CD | CT02.2.1 Sistema de gestión de contraseñas | Planeación y Sistemas de Información | Política de Seguridad de Información | Publicación en la página web |
| R3c: a servidores y estaciones de trabajo. | ALTO | CP | CT03.1.5 Política de escritorio limpio y pantalla limpia | Sistemas de Información | Política de Seguridad de Información | Publicación en la página web |
| | ALTO | CP | CT02.1.2 Política sobre el uso de los servicios de red | Sistemas de Información | * Política de Acceso * Auditorías de seguimiento | * Publicación página web * Actas de auditorías de seguimiento * Solicitudes de Servicio técnico |
| R4: Perdida de información incluye falla sísmica, falla de sistema / Daño disco duro o desconocimiento y falta de capacitación de los usuarios: | ALTO | CP | CT01.1.1 Políticas para la seguridad de la información | Comité Antitrámites y GD | Política de Seguridad de Información | Publicación en la página web |
| R4a: a dispositivos de la red. | ALTO | CC | CT03.1.2 Servicios de suministro | Sistemas de Información | Bitácora de pruebas realizadas regularmente para verificar funcionamiento correcto de las UPS | Suministro de UPS para evitar daños en los dispositivos de red |
| R4b: a servidores y estaciones de trabajo. | ALTO | CS | CT03.1.4 Retiro de activos | Sistemas de Información | * Política específica de estaciones de trabajo * Auditorías de seguimiento | * Publicación en la página web * Actas de auditoría |
| R5: Desconocer los riesgos de afectar: | ALTO | CP | CT01.1.1 Políticas para la seguridad de la información | Comité Antitrámites y GD | Política de Seguridad de Información | Publicación en la página web |
| | ALTO | CP | CT03.1.5 Política de escritorio limpio y pantalla limpia | Sistemas de Información | Política de Seguridad de Información | Publicación en la página web |
| R5a: los servidores. | ALTO | CC | CT03.1.2 Servicios de suministro | Sistemas de Información | Bitácora de pruebas realizadas regularmente para verificar funcionamiento correcto de las UPS | Suministro de UPS para evitar daños en los dispositivos de red |
| R5b: estaciones de trabajo. | ALTO | CP | CT03.1.3 Mantenimiento de equipos | Sistemas de Información | * Política específica de estaciones de trabajo * Solicitudes de servicio técnico | * Publicación en la página web * Calificación por parte de los usuarios de los servicios técnicos |





| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 73 de 95</p> |

Ilustración 15 Valoración del Riesgo (Continuación)

| RIESGO | VALORACIÓN | | | | | DISMINUIR | | RIESGO RESIDUAL | |
|---|---|---|--|--|---------------|------------------------------------|---------------------------------|--------------------|----------------------|
| | HERRAMIENTA PARA EJERCER EL CONTROL | PUNTAJE HERRAMIENTA PARA EJERCER EL CONTROL | HERRAMIENTA SEGUIMIENTO AL CONTROL | PUNTAJE HERRAMIENTA SEGUIMIENTO AL CONTROL | PUNTAJE FINAL | Rango de Calificación de Controles | CANTIDAD DE NIVELES A DISMINUIR | NUEVA CALIFICACION | MEDIDAS DE RESPUESTA |
| R3: Falla de Seguridad incluye robo, hurto, Intrusión Afectación por Virus o Ejecución no autorizado de programas: | Posee una herramienta para ejercer el control. | 15 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 30 | Entre 0-50 | 0 | ALTO | EVITAR EL RIESGOS |
| | Se ha demostrado en el tiempo que lleva la herramienta ser efectiva | 60 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 75 | Entre 51-75 | 1 | MEDIO | EVITAR EL RIESGOS |
| | Posee una herramienta para ejercer el control. | 15 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 30 | Entre 0-50 | 0 | ALTO | EVITAR EL RIESGOS |
| R3a: a portales web | Posee una herramienta para ejercer el control. | 15 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 30 | Entre 0-50 | 0 | ALTO | EVITAR EL RIESGOS |
| R3b: a firma digital. | Posee una herramienta para ejercer el control | 15 | Están definidos los responsables de la ejecución del control y del seguimiento | 0 | 0 | Entre 0-50 | 0 | ALTO | EVITAR EL RIESGOS |
| R3c: a servidores y estaciones de trabajo. | Posee una herramienta para ejercer el control. | 15 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 30 | Entre 0-50 | 0 | ALTO | EVITAR EL RIESGOS |
| | Posee una herramienta para ejercer control con manuales instructivos o procedimientos | 30 | La frecuencia de la ejecución del control y seguimiento es adecuada | 40 | 70 | Entre 51-75 | 1 | BAJO | ACEPTAR EL RIESGO |
| R4: Perdida de información incluye falla sísmica, falla de sistema / Daño disco duro o desconocimiento y falta de capacitación de los usuarios: | Posee una herramienta para ejercer el control. | 15 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 30 | Entre 0-50 | 0 | ALTO | EVITAR EL RIESGOS |
| R4a: a dispositivos de la red. | Se ha demostrado en el tiempo que lleva la herramienta ser efectiva | 60 | La frecuencia de la ejecución del control y seguimiento es adecuada | 40 | 100 | Entre 76-100 | 2 | BAJO | ACEPTAR EL RIESGO |
| R4b: a servidores y estaciones de trabajo. | Posee una herramienta para ejercer control con manuales instructivos o procedimientos | 30 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 45 | Entre 0-50 | 0 | ALTO | EVITAR EL RIESGOS |
| R5: Desconocer los riesgos de afectar: | Posee una herramienta para ejercer el control. | 15 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 30 | Entre 0-50 | 0 | ALTO | EVITAR EL RIESGOS |
| | Posee una herramienta para ejercer el control. | 15 | Están definidos los responsables de la ejecución del control y del seguimiento | 15 | 30 | Entre 0-50 | 0 | ALTO | EVITAR EL RIESGOS |
| R5a: los servidores. | Se ha demostrado en el tiempo que lleva la herramienta ser efectiva | 60 | La frecuencia de la ejecución del control y seguimiento es adecuada | 40 | 100 | Entre 76-100 | 2 | BAJO | ACEPTAR EL RIESGO |
| R5b: estaciones de trabajo. | Se ha demostrado en el tiempo que lleva la herramienta ser efectiva | 60 | La frecuencia de la ejecución del control y seguimiento es adecuada | 40 | 100 | Entre 76-100 | 2 | BAJO | ACEPTAR EL RIESGO |



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 74 de 95</p> |

6. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Ilustración 16. Plan de Tratamiento de los riesgos

| RIESGO | RIESGO INHERENTE | Controles | RIESGO RESIDUA | OPCIONES DE MANEJO | ACCIONES | RESPONSABLE | FECHA INICIO | FECHA FINAL | INDICADOR |
|--|------------------|---|----------------|--------------------|---|---|---------------|---------------|--|
| R1: Falla de Seguridad incluye robo, hurto, Intrusión Afectación por Virus o Ejecución no autorizado de programas: | MEDIO | CT01.1.1 Políticas para la seguridad de la información | MEDIO | EVITAR EL RIESGOS | * Mantener publicada la política de seguridad * Socializar la política de seguridad a los funcionarios tanto de planta como de contrato | Comité Antitrámites y GD | Vigencia 2021 | Vigencia 2022 | Indicador01 Implementación de las políticas de seguridad de la información |
| | MEDIO | CT01.1.2 Revisión de las políticas para seguridad de la información | BAJO | ACEPTAR EL RIESGO | * Establecer en el comité periodicidad para su respectiva revisión * Establecer auditorías para plantear mejoras | Control Interno y Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador02 Cobertura de la política |
| R1a: a documentos | MEDIO | CT04.1.1 Respaldo de información | MEDIO | EVITAR EL RIESGOS | * Socializar la política de almacenamiento * Establecer procedimiento de respaldo de información * Implementar herramientas tecnológicas que permita la sistematización de respaldo de información | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador11 Implementación de política de almacenamiento de información |
| | MEDIO | CT03.1.1 Ubicación y protección de los equipos | MEDIO | REDUCIR EL RIESGOS | * Instalar antivirus en la infraestructura tecnológica * Realizar monitoreos | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador06 Implementación de antivirus |
| R1b: a dispositivos de la red. | MEDIO | CT02.1.2 Política sobre el uso de los servicios de red | BAJO | ACEPTAR EL RIESGO | * Dar monitoreo a la aplicación de controles * Dar seguimiento a la implementación de la política de uso de servicios de red | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador04 Acceso controlado a los servicios de red |
| R1c: a medios de almacenamiento. | MEDIO | CT04.1.1 Respaldo de información | MEDIO | EVITAR EL RIESGOS | * Socializar la política de almacenamiento * Establecer procedimiento de respaldo de información * Implementar herramientas tecnológicas que permita la sistematización de respaldo de información | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador11 Implementación de política de almacenamiento de información |
| R1d: a telefonía IP. | MEDIO | CT01.1.1 Políticas para la seguridad de la información | MEDIO | EVITAR EL RIESGOS | * Mantener publicada la política de seguridad * Socializar la política de seguridad a los funcionarios tanto de planta como de contrato | Comité Antitrámites y GD | Vigencia 2021 | Vigencia 2022 | Indicador01 Implementación de las políticas de seguridad de la información |
| | MEDIO | CT03.1.1 Ubicación y protección de los equipos | MEDIO | REDUCIR EL RIESGOS | * Instalar antivirus en la infraestructura tecnológica * Realizar monitoreos | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador06 Implementación de antivirus |
| R2: Perdida de información: | MEDIO | CT04.1.1 Respaldo de información | MEDIO | EVITAR EL RIESGOS | * Socializar la política de almacenamiento * Establecer procedimiento de respaldo de información * Implementar herramientas tecnológicas que permita la sistematización de respaldo de información | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador11 Implementación de política de almacenamiento de información |
| R2a: por manejo inadecuado de contraseñas. | MEDIO | CT02.2.1 Sistema de gestión de contraseñas | MEDIO | EVITAR EL RIESGOS | * El procedimiento de sistema de gestión de contraseñas se incluyó en las Políticas de Seguridad Informática, se encuentra pendiente para su presentación y aprobación en el primer comité de Gestión y desempeño 2021 Planeación incorporar en el Sistema Integrado de Gestión * Bloqueo de pantallas por inactividad | Planeación y Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador05 Contraseñas establecidas |
| R2b: por uso de software no legal. | MEDIO | CT04.2.1 Restricciones sobre la instalación de software | MEDIO | REDUCIR EL RIESGOS | * Socializar la política de seguridad * Bloqueo de páginas web específicas * Monitoreos mensuales a los equipos de cómputo | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador12 Restricciones establecidas |

Fuente: Elaboración propia

Av. 0 Calle 10 Edificio Rosetal Oficina 311. Cúcuta - Norte de Santander.
Teléfonos: 5892105 Ext. 240 Email: sistemasdeinformacion@ids.gov.co
www.ids.gov.co



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 75 de 95</p> |



Ilustración 17 Plan de Tratamiento de los riesgos (Continuación)

| RIESGO | RIESGO INHERENTE | Controles | RIESGO RESIDUO | OPCIONES DE MANEJO | ACCIONES | RESPONSABLE | FECHA INICIO | FECHA FINAL | INDICADOR |
|---|------------------|---|----------------|--------------------|--|---|---------------|---------------|--|
| R3: Falta de Seguridad incluye robo, hurto, Intrusión Afectación por Virus o Ejecución no autorizado de programas: | ALTO | CT01.1.1 Políticas para la seguridad de la información | ALTO | EVITAR EL RIESGOS | * Mantener publicada la política de seguridad * Intensificar la socialización la política de seguridad a los funcionarios tanto de planta como de contrato * Inducción al personal nuevo | Comité Antitrámite s y GD | Vigencia 2021 | Vigencia 2022 | Indicador01 Implementación de las políticas de seguridad de la información |
| | ALTO | CT01.1.2 Revisión de las políticas para seguridad de la información | MEDIO | EVITAR EL RIESGOS | * Mantener publicada la política de seguridad * Socializar la política de seguridad a los funcionarios tanto de planta como de contrato * Establecer auditorías para plantear mejoras | Control Interno y Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador02 Cobertura de la política |
| | ALTO | CT02.1.1 Política de control de acceso | ALTO | EVITAR EL RIESGOS | * Intensificar las medidas de control de acceso * Dar monitoreo frecuentes para su aplicabilidad * Implementar herramientas tecnológicas de red que permita la implementación de controles | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador03 Establecimiento de control de acceso |
| R3a: a portales web | ALTO | CT02.1.1 Política de control de acceso | ALTO | EVITAR EL RIESGOS | * Intensificar las medidas de control de acceso * Dar monitoreo frecuentes para su aplicabilidad * Implementar herramientas tecnológicas de red que permita la implementación de controles | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador03 Establecimiento de control de acceso |
| R3b: a firma digital. | ALTO | CT02.2.1 Sistema de gestión de contraseñas | ALTO | EVITAR EL RIESGOS | * El procedimiento de sistema de gestión de contraseñas se incluyó en las Políticas de Seguridad Informática, se encuentra pendiente para su presentación y aprobación en el primer comité de Gestión y desempeño 2021 * Planeación incorporar en el Sistema Integrado de Gestión | Planeación y Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador05 Contraseñas establecidas |
| R3c: a servidores y estaciones de trabajo. | ALTO | CT03.1.5 Política de escritorio limpio y pantalla limpia | ALTO | EVITAR EL RIESGOS | * Establecer jornadas de formación durante el año para los antiguos. * Realizar inducción a los nuevos funcionarios | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador10 Formación en buenas practicas |
| | ALTO | CT02.1.2 Política sobre el uso de los servicios de red | BAJO | ACEPTAR EL RIESGO | * Dar monitoreo a la aplicación de controles * Dar seguimiento a la implementación de la política de uso de servicios de red | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador04 Acceso controlado a los servicios de red |
| R4: Perdida de información incluye falla sísmica, falla de sistema / Daño disco duro o desconocimiento y falta de capacitación de los usuarios: | ALTO | CT01.1.1 Políticas para la seguridad de la información | ALTO | EVITAR EL RIESGOS | * Mantener publicada la política de seguridad * Intensificar la socialización la política de seguridad a los funcionarios tanto de planta como de contrato * Inducción al personal nuevo | Comité Antitrámite s y GD | Vigencia 2021 | Vigencia 2022 | Indicador01 Implementación de las políticas de seguridad de la información |
| R4a: a dispositivos de la red. | ALTO | CT03.1.2 Servicios de suministro | BAJO | ACEPTAR EL RIESGO | * Mantener funcional las UPS | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador07 Respaldo de suministro de energía a los equipos de red |
| R4b: a servidores y estaciones de trabajo. | ALTO | CT03.1.4 Retiro de activos | ALTO | EVITAR EL RIESGOS | * Intensificar los monitoreos * Aplicar sanciones por violación de las políticas de seguridad | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador09 Grado de retiro de activos no autorizados |
| R5: Desconocer los riesgos de afectar: | ALTO | CT01.1.1 Políticas para la seguridad de la información | ALTO | EVITAR EL RIESGOS | * Mantener publicada la política de seguridad * Intensificar la socialización la política de seguridad a los funcionarios tanto de planta como de contrato * Inducción al personal nuevo | Comité Antitrámite s y GD | Vigencia 2021 | Vigencia 2022 | Indicador01 Implementación de las políticas de seguridad de la información |
| | ALTO | CT03.1.5 Política de escritorio limpio y pantalla limpia | ALTO | EVITAR EL RIESGOS | * Establecer jornadas de formación durante el año para los antiguos. * Realizar inducción a los nuevos funcionarios | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador10 Formación en buenas practicas |
| R5a: los servidores. | ALTO | CT03.1.2 Servicios de suministro | BAJO | ACEPTAR EL RIESGO | * Mantener funcional las UPS | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador07 Respaldo de suministro de energía a los equipos de red |
| R5b: estaciones de trabajo. | ALTO | CT03.1.3 Mantenimiento de equipos | BAJO | ACEPTAR EL RIESGO | * Mantener el servicio técnico fortalecido | Sistemas de Información | Vigencia 2021 | Vigencia 2022 | Indicador08 Seguimiento de solicitudes |

Fuente. Elaboración propia



Av. 0 Calle 10 Edificio Rosetal Oficina 311. Cúcuta - Norte de Santander.
Teléfonos: 5892105 Ext. 240 Email: sistemasdeinformacion@ids.gov.co
www.ids.gov.co.

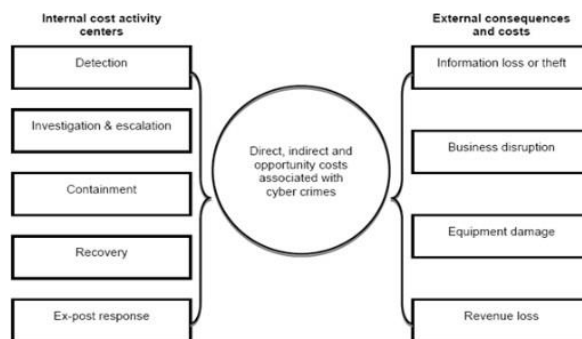
| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 76 de 95</p> |

6.1. Valoración De Incidentes – Modelo Ponemon

Extraído del objeto de aprendizaje (EAN, Objeto de Aprendizaje Atención de incidentes de seguridad informática- Algunos conceptos básicos, 2016) los incidentes de seguridad informática son:

- Según Schultz: son eventos adversos contra la seguridad en sistemas de cómputo y redes de computadores y un evento es cualquier cosa observable que ocurra en un computador o una red y que incluye las caídas de sistema, inundación de paquetes en la red, acceso no autorizado, modificación no autorizada de archivos y documentos, código malicioso y destrucción de datos.
- Según RFC2828 Internet Security Glossary: es un evento de relevante a la seguridad del sistema en el cual se vulnera o desobedece una política de seguridad.
- Según Mandia y Prosis: son aquellos que interrumpen los procedimientos de operación normal y precipitan un nivel de crisis. Se caracterizan por intensa presión, premura en el tiempo y restricciones de recursos.



Ilustración 18 Aspectos a tener en cuenta modelo Ponemon Institute



Tomado de: Ponemon Institute, 2010. First Annual Cost of Cybercrime Study, US Companies

Fuente. Tomado del ambiente de aprendizaje (EAN, Objeto de Aprendizaje Atención de incidentes de seguridad informática- Algunos conceptos básicos, 2016)



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 77 de 95</p> |

A continuación se relaciona unos valores basados en supuestos para el Instituto Departamental de Salud de Norte de Santander, aunque es una entidad pública y no se refleja en costos, si representa un gasto a la Entidad y pérdida de credibilidad de la Entidad ante la comunidad Nortesantandereana y ante los entes de Control Departamentales y Nacionales.

Tabla 23 Valoración de costos

| Valoración de los costos internos del modelo de negocio | |
|---|--------------------|
| Descripción | Valor Hora /Hombre |
| Ingeniero de Soporte | 10.000 |
| Líder de Sistemas de Información | 15.000 |
| Valoración de costos externos del modelo de negocio | |
| Descripción | Valor por hora |
| Tiempo en Detectar el Incidente | 500.000 |
| Tiempo en Investigar el Incidente | 200.000 |
| Tiempo para Contrarrestar el Incidente | 100.000 |
| Información Adicional | Valor |
| Cantidad de registro, que se vieron comprometidos | 10.000.000 |
| Porcentaje de clientes insatisfechos, por perdida de la información | 15% |
| Reserva para mantener la reputación de la empresa | 10.000.000 |

Fuente. Elaboración propia

Tabla 24 Diez (10) Incidentes de seguridad según Kaspersky.

| INCIDENTES |
|---|
| Virus / Malware / Troyanos |
| Uso inadecuado de los recursos de TI por parte de los empleados |
| Perdida de datos/por exposición a ataques dirigidos - Acciones maliciosas de personal interno |
| Incidente que involucren dispositivos no informáticos (Externos) conectados |
| Incidente que afecta la infraestructura TI alojada por un tercero |
| Incidente que afecta a los proveedores con los que compartimos |
| Perdida física de equipo que contenga datos |
| Perdida de datos/por exposición a ataques dirigidos |

Fuente. Elaboración propia basada en Kaspersky (2017)





| | | |
|---|-------------------------------------|--|
|  INSTITUTO DEPARTAMENTAL DE SALUD <small>NORTE DE SANTANDER</small> | DIRECCIONAMIENTO ESTRATEGICO |  Gobernación de Norte de Santander <small>Instituto Departamental de Salud</small> |
| Código: F-DE-PE05-04 Versión: 05 | COMUNICACION INTERNA | Página 78 de 95 |

Ilustración 19 Valores de los costos internos

| INCIDENTES SEGUN KASPERSKY | Tipo de personal requerido | Detención | | Investigación y escalamiento | | Contención | | Recuperación | | Respuesta Post | |
|---|----------------------------------|-----------|----------------|------------------------------|----------------|------------|----------------|--------------|----------------|----------------|---------------|
| | | Horas | Costo | Horas | Costo | Horas | Costo | Horas | Costo | Horas | Costo |
| Virus / Malware / Troyanos | Ingeniero de Soporte | 2 | 20.000 | 1 | 10.000 | 1 | 10.000 | 5 | 50.000 | 1 | 10.000 |
| | Líder de Sistemas de Información | 1 | 15.000 | 1 | 15.000 | 1 | 15.000 | 3 | 45.000 | 3 | 45.000 |
| | Total | 3 | 35.000 | 2 | 25.000 | 2 | 25.000 | 8 | 95.000 | 4 | 55.000 |
| Uso inadecuado de los recursos de TI por parte de los empleados | Ingeniero de Soporte | 2 | 20.000 | 2 | 20.000 | 2 | 20.000 | 1 | 10.000 | 2 | 20.000 |
| | Líder de Sistemas de Información | 2 | 30.000 | 2 | 30.000 | 2 | 30.000 | 1 | 15.000 | 2 | 30.000 |
| | Total | 4 | 50.000 | 4 | 50.000 | 4 | 50.000 | 2 | 25.000 | 4 | 50.000 |
| Acciones maliciosas de personal interno | Ingeniero de Soporte | 5 | 10.000 | 2 | 20.000 | 3 | 30.000 | 2 | 20.000 | 1 | 10.000 |
| | Líder de Sistemas de Información | 8 | 120.000 | 2 | 30.000 | 3 | 45.000 | 2 | 30.000 | 1 | 15.000 |
| | Total | 13 | 130.000 | 4 | 50.000 | 6 | 75.000 | 4 | 50.000 | 2 | 25.000 |
| Pérdida de datos/por exposición a ataques dirigidos | Ingeniero de Soporte | 1 | 10.000 | 2 | 20.000 | 2 | 10.000 | 2 | 20.000 | 1 | 10.000 |
| | Líder de Sistemas de Información | 1 | 15.000 | 2 | 30.000 | 2 | 15.000 | 2 | 30.000 | 1 | 15.000 |
| | Total | 2 | 25.000 | 4 | 50.000 | 4 | 25.000 | 4 | 50.000 | 2 | 25.000 |
| Incidente que involucren dispositivos no informáticos (Externos) conectados | Ingeniero de Soporte | 1 | 10.000 | 3 | 30.000 | 5 | 50.000 | 2 | 20.000 | 1 | 10.000 |
| | Líder de Sistemas de Información | 1 | 15.000 | 3 | 45.000 | 5 | 75.000 | 2 | 30.000 | 1 | 15.000 |
| | Total | 2 | 25.000 | 6 | 75.000 | 10 | 125.000 | 4 | 50.000 | 2 | 25.000 |
| Incidente que afecta la infraestructura TI alojada por un tercero | Ingeniero de Soporte | 2 | 20.000 | 3 | 30.000 | 2 | 20.000 | 2 | 20.000 | 1 | 10.000 |
| | Líder de Sistemas de Información | 2 | 30.000 | 3 | 45.000 | 2 | 30.000 | 2 | 30.000 | 1 | 15.000 |
| | Total | 4 | 50.000 | 6 | 75.000 | 4 | 50.000 | 4 | 50.000 | 2 | 25.000 |
| Incidente que afecta a los proveedores con los que compartimos | Ingeniero de Soporte | 2 | 20.000 | 2 | 20.000 | 2 | 20.000 | 2 | 20.000 | 1 | 10.000 |
| | Líder de Sistemas de Información | 2 | 30.000 | 2 | 30.000 | 2 | 30.000 | 2 | 30.000 | 1 | 15.000 |
| | Total | 4 | 50.000 | 4 | 50.000 | 4 | 50.000 | 4 | 50.000 | 2 | 25.000 |
| Pérdida física de equipo que contenga datos | Ingeniero de Soporte | 2 | 20.000 | 2 | 20.000 | 1 | 10.000 | 1 | 10.000 | 1 | 10.000 |
| | Líder de Sistemas de Información | 2 | 30.000 | 2 | 30.000 | 1 | 15.000 | 1 | 15.000 | 1 | 15.000 |
| | Total | 4 | 50.000 | 4 | 50.000 | 2 | 25.000 | 2 | 25.000 | 2 | 25.000 |
| Pérdida de datos/por exposición a ataques dirigidos | Ingeniero de Soporte | 3 | 30.000 | 5 | 50.000 | 5 | 50.000 | 2 | 20.000 | 2 | 20.000 |
| | Líder de Sistemas de Información | 3 | 45.000 | 5 | 75.000 | 5 | 75.000 | 2 | 30.000 | 2 | 30.000 |
| | Total | 6 | 75.000 | 10 | 125.000 | 10 | 125.000 | 4 | 50.000 | 4 | 50.000 |
| Fuga electrónica de datos de los sistemas internos | Ingeniero de Soporte | 1 | 10.000 | 3 | 30.000 | 4 | 40.000 | 4 | 40.000 | 2 | 20.000 |
| | Líder de Sistemas de Información | 1 | 15.000 | 3 | 45.000 | 4 | 60.000 | 4 | 60.000 | 2 | 30.000 |
| | Total | 2 | 25.000 | 6 | 75.000 | 8 | 100.000 | 8 | 100.000 | 4 | 50.000 |

Fuente. Elaboración propia





| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 79 de 95</p> |

Tabla 25 Valores de los costos externos

| INCIDENTE | Pérdida o robo de Información Costo Total | Interrupción del Negocio | | | Daños a los Equipos | |
|---|--|--|-------|-----------|---|-------------|
| | | Tipo de tiempos | Horas | Costo | Descripción | Costo |
| Virus / Malware / Troyanos | 11.500.000,00 | Tiempo en Detectar el Incidente | 1 | 500.000 | Reparación de software infectado | 5.000.000 |
| | | Tiempo en Investigar el Incidente | 2 | 400.000 | | |
| | | Tiempo para Contrarrestar el Incidente | 2 | 200.000 | | |
| | | Total | | 1.100.000 | | |
| Uso inadecuado de los recursos de TI por parte de los empleados | | Tiempo en Detectar el Incidente | 4 | 2.000.000 | Reparación de recursos TIC, lo debe asumir el empleado | 0 |
| | | Tiempo en Investigar el Incidente | 3 | 600.000 | | |
| | | Tiempo para Contrarrestar el Incidente | 4 | 400.000 | | |
| | | Total | | 3.000.000 | | |
| Acciones maliciosas de personal interno | | Tiempo en Detectar el Incidente | 16 | 8.000.000 | Implementar herramientas de LOG de seguridad | 50.000.000 |
| | | Tiempo en Investigar el Incidente | 4 | 800.000 | | |
| | | Tiempo para Contrarrestar el Incidente | 4 | 400.000 | | |
| | | Total | | 8.000.000 | | |
| Pérdida de datos/por exposición a ataques dirigidos | | Tiempo en Detectar el Incidente | 4 | 2.000.000 | Adquisición de firewall robusto que permita la protección de los datos | 100.000.000 |
| | | Tiempo en Investigar el Incidente | 8 | 1.600.000 | | |
| | | Tiempo para Contrarrestar el Incidente | 4 | 400.000 | | |
| | | Total | | 4.000.000 | | |
| Incidente que involucren dispositivos no informáticos (Externos) conectados | | Tiempo en Detectar el Incidente | 3 | 1.500.000 | Adquisición de herramienta informática que permita el control de los dispositivos | 50.000.000 |
| | | Tiempo en Investigar el Incidente | 2 | 400.000 | | |
| | | Tiempo para Contrarrestar el Incidente | 8 | 800.000 | | |
| | | Total | | 2.700.000 | | |
| Incidente que afecta la infraestructura TI alojada por un tercero | | Tiempo en Detectar el Incidente | 8 | 4.000.000 | Especificaciones técnicas claras contractuales | 10.000.000 |
| | | Tiempo en Investigar el Incidente | 8 | 1.600.000 | | |
| | | Tiempo para Contrarrestar el Incidente | 8 | 800.000 | | |
| | | Total | | 6.400.000 | | |
| Incidente que afecta a los proveedores con los que compartimos | | Tiempo en Detectar el Incidente | 8 | 4.000.000 | Implementar sistema de seguridad a la plataforma TIC | 100.000.000 |
| | | Tiempo en Investigar el Incidente | 8 | 1.600.000 | | |
| | | Tiempo para Contrarrestar el Incidente | 4 | 400.000 | | |
| | | Total | | 6.000.000 | | |
| Pérdida física de equipo que contenga datos | | Tiempo en Detectar el Incidente | 2 | 1.000.000 | Codificación de los equipos utilizando Internet de las Cosas | 300.000.000 |
| | | Tiempo en Investigar el Incidente | 8 | 1.600.000 | | |
| | | Tiempo para Contrarrestar el Incidente | 1 | 100.000 | | |
| | | Total | | 2.700.000 | | |
| Pérdida de datos/por exposición a ataques dirigidos | | Tiempo en Detectar el Incidente | 8 | 4.000.000 | Herramienta de protección de datos y procedimientos definidos para protección y recuperación de datos | 150.000.000 |
| | | Tiempo en Investigar el Incidente | 4 | 800.000 | | |
| | | Tiempo para Contrarrestar el Incidente | 8 | 800.000 | | |
| | | Total | | 5.600.000 | | |
| Fuga electrónica de datos de los sistemas internos | | Tiempo en Detectar el Incidente | 8 | 4.000.000 | Configuración de los dispositivos de red para el control de los sistemas de información | 50.000.000 |
| | | Tiempo en Investigar el Incidente | 4 | 800.000 | | |
| | | Tiempo para Contrarrestar el Incidente | 8 | 800.000 | | |
| | | Total | | 5.600.000 | | |

Fuente. Elaboración propia





| | | |
|---|-------------------------------------|--|
|  INSTITUTO DEPARTAMENTAL DE SALUD <small>NORTE DE SANTANDER</small> | DIRECCIONAMIENTO ESTRATEGICO |  Gobernación de Norte de Santander <small>Instituto Departamental de Salud</small> |
| Código: F-DE-PE05-04 Versión: 05 | COMUNICACION INTERNA | Página 80 de 95 |

Tabla 26 Resumen de costos basado en Modelo Ponemon Institute

| INCIDENTE | Detención | Investigación y escalamiento | Contención | Recuperación | Respuesta Post | TOTAL COSTOS INTERNOS | Pérdida o robo de Información | Interrupción del Negocio | Daños a los Equipos |
|---|-----------|------------------------------|------------|--------------|----------------|-----------------------|-------------------------------|--------------------------|---------------------|
| Virus / Malware / Troyanos | 30.000 | 45.000 | 30.000 | 30.000 | 15.000 | 150.000 | 11.500.000 | 1.100.000 | 5.000.000 |
| Uso inadecuado de los recursos de TI por parte de los empleados | 50.000 | 50.000 | 50.000 | 50.000 | 25.000 | 225.000 | | 3.000.000 | 0 |
| Acciones maliciosas de personal interno | 50.000 | 50.000 | 25.000 | 25.000 | 25.000 | 175.000 | | 9.200.000 | 50.000.000 |
| Perdida de datos/por exposición a ataques dirigidos | 25.000 | 50.000 | 25.000 | 50.000 | 25.000 | 175.000 | | 4.000.000 | 100.000.000 |
| Incidente que involucren dispositivos no informáticos (Externos) conectados | 25.000 | 75.000 | 125.000 | 50.000 | 25.000 | 300.000 | | 2.700.000 | 50.000.000 |
| Incidente que afecta la infraestructura TI alojada por un tercero | 50.000 | 75.000 | 50.000 | 50.000 | 25.000 | 250.000 | | 6.400.000 | 10.000.000 |
| Incidente que afecta a los proveedores con los que compartimos | 50.000 | 50.000 | 50.000 | 50.000 | 25.000 | 225.000 | | 6.000.000 | 100.000.000 |
| Perdida física de equipo que contenga datos | 50.000 | 50.000 | 25.000 | 25.000 | 25.000 | 175.000 | | 2.700.000 | 300.000.000 |
| Perdida de datos/por exposición a ataques dirigidos | 75.000 | 125.000 | 125.000 | 50.000 | 50.000 | 425.000 | | 5.600.000 | 150.000.000 |
| Fuga electrónica de datos de los sistemas internos | 25.000 | 75.000 | 100.000 | 100.000 | 50.000 | 350.000 | | 5.600.000 | 50.000.000 |

Fuente. Elaboración propia





| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 81 de 95</p> |

7. ANALISIS DE AMENAZAS Y RIESGOS EMERGENTES EN SEGURIDAD DE LA INFORMACION

Los riesgos y amenazas hacen parte de nuestro entorno laboral que va a la mano tanto la administración como de la evolución de las tecnologías; lo que ha generado la expedición de modelos para la gestión de la seguridad de la información que permita mitigar los riesgos que afectan estratégicamente a una organización, que contribuya al apoyo de la toma de decisiones y de ésta manera garantizar la continuidad del negocio; de acuerdo a la ISO 27000 (2012) Sistema de Gestión de Seguridad de la Información ayuda a establecer políticas y procedimientos relacionados a los objetivos de negocio de la organización, manteniendo un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Sin embargo, se debe tener en cuenta que la dinámica de las organizaciones que tenemos hoy en día ha cambiado radicalmente en la última década, teniendo en cuenta que la tecnología es versátil y cambia constantemente a pasos agigantados convirtiendo las empresas administradas tradicionalmente en empresas digitales y de ésta misma manera los riesgos son variables y han evolucionado, por ello, los responsables de la seguridad de la información deben desarrollar una competencia estratégica para mantenerse alerta y anticiparse a posibles fallos, teniendo en cuenta cuatro elementos: la información, las estrategias y metas del negocio, los fundamentos de seguridad y la administración de los riesgos; logrando escenarios predictivos y preventivos que custodie a la organización frente a las amenazas y riesgos emergentes tanto en el entorno interno como externo (Inseguridad de la Información: Una Visión Estratégica, 2013, págs. 19-20).

La nueva era de las empresas digitales han propuesto nuevos retos, tanto en la administración de la información como en la seguridad de la misma, teniendo en cuenta





| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 82 de 95</p> |

que la información en la actualidad es instantánea y de fácil acceso por las personas a través del internet, en las redes sociales en equipos de cómputo y dispositivos móviles; el mundo empresarial y personal está totalmente inmerso en la tecnología, esto ha abierto nuevos panoramas de incertidumbre para la seguridad de la información lo que disminuye la aceptación de la gestión del riesgo tradicional, por tanto, es indispensable herramientas que permitan “ampliar la capacidad de conocimiento del entorno y facilitar la toma de decisiones” (Cano M., La ventana de AREM. Una herramienta estratégica y táctica para visualizar la incertidumbre, 2014). Teniendo en cuenta que la nueva realidad de negocios aumenta el nivel de riesgo por la exposición, colaboración, entrega, intercambio y flujo de información, por tanto, nada es predecible y la información se debe visualizar de manera dinámica analizando todos los entornos, entendiendo el nuevo ecosistema digital (Cano M., 2014)

Finalmente el Dr. Cano quien manifiesta en su conferencia (Pronósticos de seguridad de la información 2017. Cinco imperativos para avanzar en un mundo digitalmente modificado, 2017) que cada día existen mayores retos para detectar ataques porque se deben tener en cuenta las nuevas tecnologías que son productos y servicios digitalmente modificados, el mayor flujo de datos personales y corporativos que tienen una interacción directa con las personas, la acelerada convergencia tecnológica con el fin de generar mayor eficiencia y efectividad en las operaciones y, finalmente el incremento de la movilidad y mayor control de la tecnología por parte de las personas, por tal razón, se debe hacer mayor énfasis en elementos claves que se deben monitorear constantemente tales como ataque “sin archivos”, infiltraciones con cifrado, ataques bajo el sistema operativo y, finalmente, Shell y control remoto, los cuales, se desarrollan en la computación en la nube, la virtualización, la computación móvil y las redes sociales, teniendo en cuenta lo anterior expuesto, se hace necesario un cambio de paradigma desde las directivas hasta el personal para confrontar la nueva forma de operar y lograr la continuidad del negocio y finalmente, alcanzar



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 83 de 95</p> |



ventaja competitiva; lo que implica una nueva manera de enfrentar las amenazas y riesgos emergentes ya que existirán unas incertidumbres y ambigüedades constantes alrededor de los ciber riesgos y análisis de diferentes escenarios.

7.1. Análisis de incertidumbres

| | Lo que conoce la Organización | Lo que desconoce la Organización |
|------------------------------------|---|--|
| Lo que conoce el entorno | Falla de Seguridad, Robo, Hurto, Intrusión Afectación por Virus, Ejecución no autorizado de programas, Manejo inadecuado de contraseñas, Uso de software no legal, falla sísmica, falla de sistema, Daño disco duro, Desconocimiento y falta de capacitación de los usuarios, Desconocer los riesgos de afectar los equipos informáticos. | Ataques distribuidos, Hacking, Amenaza Persistente Avanzada, Malware, Ataques al firmware, Pharming, iframe. |
| | Conocidos | Latentes |
| Lo que desconoce el entorno | Fuga de información epidemiológica, Ataques dirigidos a los Sistemas de Información del IDS, Hacktivismo, Phishing, falla en infraestructura física, | Ciber terrorismo, Ciber espionaje, Ciber conflictos, desastres naturales, |

Fuente. Elaboración propia basada en modelo (Cano M., 2014)



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 84 de 95</p> |

CONCLUSIONES

La ausencia de políticas de seguridad pone en riesgo las actividades diarias de las organizaciones y afectando la integridad, disponibilidad y confidencialidad de la información y a su vez el logro de los objetivos estratégicos.

Las políticas de seguridad demuestran la importancia que tiene la organización en proteger uno de los activos más significativos e indispensables para el desarrollo de sus actividades y la consecución de las metas.



Desde la Dirección se debe apoyar todo proceso de definición, ejecución y puesta en marcha de los sistemas de gestión de seguridad con el fin de fomentar un cambio en la cultura organizacional para la incorporación y utilización de éstas, ya que, el éxito de su aplicabilidad depende del conocimiento y el uso adecuado de las tecnologías y sistemas de información por parte de todos los empleados de la organización.

El análisis de riesgos se torna en una herramienta indispensable para establecer las medidas de prevención y control de los riesgos asociados, al entorno físico, ambiental, social, estructural en el cual desarrolla sus funciones y permite evidenciar la vulnerabilidad que sufre los datos e información e infraestructura, ante las inminentes amenazas de diferentes orígenes, también ayuda a definir o mejorar los controles que ayuden a prevenir los daños.

Con el establecimiento de controles e indicadores permite dar seguimiento y aporta al fortalecimiento de las medidas para evitar o reducir los posibles riesgos a los que se puedan enfrentar.



Con el modelo Ponemon Institute permite estimar los posibles costos tanto internos como externos ante la presencia de posibles incidentes.



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 85 de 95</p> |

Hoy en día se debe generar un cambio de paradigma para incursionar en la nueva era de las organizaciones digitales, de manera que permita confrontar las amenazas y riesgos emergentes y con una proyección de generar ventaja competitiva a través de servicios o productos digitalmente modificados.





| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 86 de 95</p> |

BIBLIOGRAFÍA

- Bueno, G., Correa, C., & Echeverry, J. I. (Marzo de 2010). *Administración de Riesgos - una visión global y moderna*. Obtenido de <https://www.colibri.udelar.edu.uy/bitstream/123456789/201/1/M-CD4026.pdf>
- Cano M., J. J. (2014). La función de seguridad de la información. Presiones actuales y emergentes desde la inseguridad de la información. *ISACA Journal Volume 6*. Obtenido de https://www.isaca.org/Journal/archives/2014/Volume-6/Documents/The-Information-Security-Function_joa_Spa_1114.pdf
- Cano M., J. J. (2014). La ventana de AREM. Una herramienta estratégica y táctica para visualizar la incertidumbre. *RECSI, Alicante*, 215-220.
- Cano Martínez, J. J. (2013). *Inseguridad de la Información: Una Visión Estratégica*. Bogotá: Alfaomega.
- Cano Martínez, J. J. (20 de enero de 2017). *Pronósticos de seguridad de la información 2017. Cinco imperativos para avanzar en un mundo digitalmente modificado*. Obtenido de ACIS: <https://www.youtube.com/watch?v=NbCmc08OBjU>
- Cano, J. (2000). Pautas y recomendaciones para elaborar políticas de seguridad informática (psi). 6.
- Comisión Nacional de Investigación Científica y Tecnológica. (2011). *Política General de Seguridad de la Información*. 2011.
- DAFP. (Septiembre de 2011). *Guía para la Administración del Riesgo*. Obtenido de <http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba>
- EAN. (2016). *Objeto de Aprendizaje Atención de incidentes de seguridad informática- Algunos conceptos básicos*. Obtenido de virtual.universidadean.edu.co: https://virtual.universidadean.edu.co/bbcswebdav/pid-415872-dt-content-rid-4686385_1/courses/PADREIMGAIFEAV/2017_C2_AVA/index.html
- Erb, M. (2015). *Matriz para el análisis del riesgo. Gestión de Riesgo en la Seguridad*. Obtenido de <https://protejete.wordpress.com>: <http://bit.ly/1P4iJog>
- Gobierno de España. (Octubre de 2012). *Metodología de análisis y gestión de riesgos de los sistemas de información*. Obtenido de <http://administracionelectronica.gob.es>: <http://bit.ly/1QJQOs4>



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 87 de 95</p> |

ICONTEC. (3 de Abril de 2006). *NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001*. Obtenido de <http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf>

ICONTEC. (16 de Enero de 2011). *ISO/IEC 27002:2005*. Obtenido de www.iso27000.es:
<http://www.iso27000.es/download/ControlesISO27002-2005.pdf>

IDS. (2017). *Instituto Departamental de Salud de Norte de Santander*. Obtenido de www.ids.gov.co

Invima. (2017). *Política de seguridad de la información*. Bogotá.

ISO. (2012). *Sistema de Gestión de la Seguridad de la Información*. Obtenido de <http://www.iso27000.es>:
http://www.iso27000.es/download/doc_sgsi_all.pdf

Kaspersky. (2017). *Incidentes de seguridad según según Kaspersky*. Obtenido de https://usblog.kaspersky.com/security_risks_report_perception/

Ministerio de Hacienda y Administraciones Públicas. (2012). *Magerit v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid: Administración electrónica.

Ministerio de Tecnologías de la Información y las Comunicaciones. (1 de Abril de 2016). *Guía de Gestión de Riesgos - Seguridad y Privacidad de la Información*. Obtenido de www.mintic.gov.co:
https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

MinTIC. (25 de mayo de 2015). *Guía de indicadores de gestión para la seguridad de información*. Obtenido de www.mintic.gov.co: https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf



MinTIC. (14 de Marzo de 2016). *Controles de Seguridad y Privacidad de la Información*. Obtenido de www.mintic.gov.co: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Procuraduría General de la Nación. (2014). *Código Disciplinario único - Ley 734 de 2002*. Obtenido de www.procuraduria.gov.co:
<https://www.procuraduria.gov.co/relatoria/media/file/CODIGODISCIPLINARIO.pdf>

Rivas Fernández, J. B. (2003). La gerencia de Información: El caso de los archivos. *Redalyc*, 3-13.



Secretaría Distrital de Salud de Bogotá. (2012). *Política de seguridad de la información de la Secretaría Distrital De Salud*. Bogotá.



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 88 de 95</p> |

Sinnexus. (2017). *Business Intelligence*. Recuperado el 01 de Mayo de 2017, de Business Intelligence:
http://www.sinnexus.com/business_intelligence/piramide_negocio.aspx



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 89 de 95</p> |

ANEXO

Anexo 1. Definición de indicadores propuestos

INDICADOR01

| | | | |
|--|-------------|--|---|
| Implementación de las políticas de seguridad de la información | | | |
| IDENTIFICADOR | Indicador01 | | |
| DEFINICIÓN | | | |
| Cumplimiento de políticas de seguridad de la información en la entidad | | | |
| OBJETIVO | | | |
| Identificar que la Dirección haya aprobado y publicado un documento de la política de seguridad de la información | | | |
| TIPO DE INDICADOR | | MEDIDA DEL INDICADOR | |
| Táctico | | Política aprobada y publicada | |
| DESCRIPCIÓN DE VARIABLES | | FORMULA | |
| ¿La entidad ha definido una política general de seguridad de la información? ¿La entidad ha publicado la política general de seguridad de la información? | | Las dos preguntas afirmativas = 1 Una o dos preguntas negativas = 0 | |
| METAS | | | |
| CUMPLE | 1 | NO CUMPLE | 0 |



Fuente. Elaboración propia basada en la Guía de Indicadores de gestión para la seguridad de la información (MinTIC, 2015) y en ISO/IEC 27002:2005 (ICONTEC, 2011)

INDICADOR02

| | | | | | |
|--|-------------|----------------------|-----------------------------|----------------------|---------|
| Cobertura de la política | | | | | |
| IDENTIFICADOR | Indicador02 | | | | |
| DEFINICIÓN | | | | | |
| La política ha sido comunicada a todos los empleados relevantes para su aplicabilidad y actualización permanente | | | | | |
| OBJETIVO | | | | | |
| Medir el grado de despliegue, adopción y actualización de la política | | | | | |
| TIPO DE INDICADOR | | | MEDIDA DEL INDICADOR | | |
| Táctico | | | Porcentaje | | |
| DESCRIPCIÓN DE VARIABLES | | | FORMULA | | |
| V1: Personal capacitado V2: Total de Personal de planta y contratado | | | V1/V2*100 | | |
| METAS | | | | | |
| MINIMA | 60-80% | SATISFACTORIA | 81-90% | SOBRESALIENTE | 91-100% |

Fuente. Elaboración propia basada en la Guía de Indicadores de gestión para la seguridad de la información (MinTIC, 2015) y en ISO/IEC 27002:2005 (ICONTEC, 2011)



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 90 de 95</p> |

INDICADOR03

| | | | |
|--|-------------|--|---|
| Establecimiento de control de acceso | | | |
| IDENTIFICADOR | Indicador03 | | |
| DEFINICION | | | |
| Se debe establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización | | | |
| OBJETIVO | | | |
| Identificar la existencia de lineamientos, normas o estándares en cuanto al control de acceso en la entidad. | | | |
| TIPO DE INDICADOR | | MEDIDA DEL INDICADOR | |
| Operativo | | Política de Control de acceso implementada | |
| DESCRIPCION DE VARIABLES | | FORMULA | |
| ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el acceso de los usuarios a sus redes de comunicaciones? ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el uso y el acceso a los sistemas de información y las aplicaciones con las que cuenta la entidad? | | Las dos preguntas afirmativas = 1 Una o dos preguntas negativas = 0 | |
| METAS | | | |
| CUMPLE | 1 | NO CUMPLE | 0 |



Fuente. Elaboración propia basada en la Guía de Indicadores de gestión para la seguridad de la información (MinTIC, 2015) y en ISO/IEC 27002:2005 (ICONTEC, 2011)

INDICADOR04

| | | | |
|--|-------------|-----------------------------|----|
| Acceso controlado a los servicios de red | | | |
| IDENTIFICADOR | Indicador04 | | |
| DEFINICION | | | |
| Se debe proveer a los usuarios de los accesos a los servicios para los que han sido expresamente autorizados a utilizar. | | | |
| OBJETIVO | | | |
| Calcular la tasa de los accesos no controlado a los servicios de red | | | |
| TIPO DE INDICADOR | | MEDIDA DEL INDICADOR | |
| Operativo | | Porcentaje | |
| DESCRIPCION DE VARIABLES | | FORMULA | |
| V3: Número de accesos no autorizados a los servicios de red V4: Total de accesos autorizados a los servicios de red | | V3/V4 | |
| METAS | | | |
| MINIMA | <10 y >6 | SATISFACTORIA | <5 |
| | | SOBRESALIENTE | 0 |

Fuente. Elaboración propia basada en la Guía de Indicadores de gestión para la seguridad de la información (MinTIC, 2015)



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 91 de 95</p> |

INDICADOR05

| Contraseñas establecidas | | | | | |
|--|-------------|----------------------|----------------------|----------------------|---------|
| IDENTIFICADOR | Indicador05 | | | | |
| DEFINICION | | | | | |
| Todos los usuarios deberían disponer de un único identificador propio para su uso personal y exclusivo. Se debería elegir una técnica de autenticación adecuada que verifique la identidad reclamada por un usuario. | | | | | |
| OBJETIVO | | | | | |
| Calcular el grado de acceso a la información con el establecimiento de contraseñas | | | | | |
| TIPO DE INDICADOR | | | MEDIDA DEL INDICADOR | | |
| Operativo | | | Porcentaje | | |
| DESCRIPCION DE VARIABLES | | | FORMULA | | |
| V5: Contraseñas establecidas V6: Total de funcionarios que deben tener contraseña | | | V5/V6*100 | | |
| METAS | | | | | |
| MINIMA | 70-80% | SATISFACTORIA | 81-89% | SOBRESALIENTE | 90-100% |



Fuente. Elaboración propia basada en la Guía de Indicadores de gestión para la seguridad de la información (MinTIC, 2015) y en ISO/IEC 27002:2005 (ICONTEC, 2011)

INDICADOR06

| Implementación de antivirus | | | | | |
|---|-------------|----------------------|----------------------|----------------------|------|
| IDENTIFICADOR | Indicador06 | | | | |
| DEFINICION | | | | | |
| Los equipos se deben proteger para reducir el riesgo de materialización de las amenazas del entorno | | | | | |
| OBJETIVO | | | | | |
| Calcular el grado de implementación de antivirus en las estaciones de trabajo | | | | | |
| TIPO DE INDICADOR | | | MEDIDA DEL INDICADOR | | |
| Operativo | | | Porcentaje | | |
| DESCRIPCION DE VARIABLES | | | FORMULA | | |
| V7: Total de quipos con antivirus V8: Total de equipos de la entidad | | | V7/V8*100 | | |
| METAS | | | | | |
| MINIMA | 80-89% | SATISFACTORIA | 90-99% | SOBRESALIENTE | 100% |

Fuente. Elaboración propia basada en la Guía de Indicadores de gestión para la seguridad de la información (MinTIC, 2015) y en ISO/IEC 27002:2005 (ICONTEC, 2011)



| | | |
|---|--|--|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 92 de 95</p> |

INDICADOR07

| | | | |
|---|-------------|-----------------------------|---|
| Respaldo de suministro de energía a los equipos de red | | | |
| IDENTIFICADOR | Indicador07 | | |
| DEFINICION | | | |
| Se deber proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de la red de comunicaciones | | | |
| OBJETIVO | | | |
| Garantizar la continuidad del servicio | | | |
| TIPO DE INDICADOR | | MEDIDA DEL INDICADOR | |
| Operativo | | Se cuenta con UPS | |
| DESCRIPCION DE VARIABLES | | FORMULA | |
| ¿La entidad cuenta con UPS para los equipos de la red de comunicaciones? | | SI=1 NO=0 | |
| METAS | | | |
| CUMPLE | 1 | NO CUMPLE | 0 |



Fuente. Elaboración propia basada en la Guía de Indicadores de gestión para la seguridad de la información (MinTIC, 2015) y en ISO/IEC 27002:2005 (ICONTEC, 2011)

INDICADOR08

| | | | |
|--|-------------|-----------------------------|---------|
| Seguimiento de solicitudes | | | |
| IDENTIFICADOR | Indicador08 | | |
| DEFINICION | | | |
| Garantizar la continuidad de los servicios informáticos atendiendo las solicitudes de servicios de soporte técnico | | | |
| OBJETIVO | | | |
| Calcular el grado de cumplimiento de atención a las solicitudes realizadas. | | | |
| TIPO DE INDICADOR | | MEDIDA DEL INDICADOR | |
| Operativo | | Porcentaje | |
| DESCRIPCION DE VARIABLES | | FORMULA | |
| V9: Total de solicitudes atendidas V10: Total de solicitudes realizadas | | V9/V10*100 | |
| METAS | | | |
| MINIMA | 60-70% | SATISFACTORIA | 71-79% |
| | | SOBRESALIENTE | 80-100% |

Fuente. Elaboración propia basada en la Guía de Indicadores de gestión para la seguridad de la información (MinTIC, 2015) y en ISO/IEC 27002:2005 (ICONTEC, 2011)



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 93 de 95</p> |

INDICADOR09

| Grado de retiro de activos no autorizados | | | | | |
|--|-------------|----------------------|-----------------------------|----------------------|----|
| IDENTIFICADOR | Indicador09 | | | | |
| DEFINICION | | | | | |
| No se debe sacar equipos, información o software fuera de la entidad sin una autorización | | | | | |
| OBJETIVO | | | | | |
| Calcular el grado de retiros de activos no autorizados | | | | | |
| TIPO DE INDICADOR | | | MEDIDA DEL INDICADOR | | |
| Operativo | | | Porcentaje | | |
| DESCRIPCION DE VARIABLES | | | FORMULA | | |
| V11: Cantidad de Equipos, información o software retirado sin autorización V12: Total de equipos, información o software de muestra | | | V11/V12*100 | | |
| METAS | | | | | |
| MINIMA | 20% | SATISFACTORIA | 10% | SOBRESALIENTE | 0% |



Fuente. Elaboración propia basada en la Guía de Indicadores de gestión para la seguridad de la información (MinTIC, 2015) y en ISO/IEC 27002:2005 (ICONTEC, 2011)

INDICADOR10

| Formación en buenas practicas | | | | | |
|---|-------------|----------------------|-----------------------------|----------------------|---------|
| IDENTIFICADOR | Indicador10 | | | | |
| DEFINICION | | | | | |
| Permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales. | | | | | |
| OBJETIVO | | | | | |
| Establecer la efectividad de la formación y sensibilización previamente definido como medio para el control de incidentes de seguridad. | | | | | |
| TIPO DE INDICADOR | | | MEDIDA DEL INDICADOR | | |
| Operativo | | | | | |
| DESCRIPCION DE VARIABLES | | | FORMULA | | |
| V13: Personal capacitado en buenas practicas V14: Total de personal de planta y contratado | | | V13/V14*100 | | |
| METAS | | | | | |
| MINIMA | 70-79% | SATISFACTORIA | 80-89% | SOBRESALIENTE | 90-100% |

Fuente. Elaboración propia basada en la Guía de Indicadores de gestión para la seguridad de la información (MinTIC, 2015) y en ISO/IEC 27002:2005 (ICONTEC, 2011)



| | | |
|---|--|---|
|  <p>INSTITUTO DEPARTAMENTAL DE SALUD NORTE DE SANTANDER</p> | <p>DIRECCIONAMIENTO ESTRATEGICO</p> |  <p>Gobernación de Norte de Santander Instituto Departamental de Salud</p> |
| <p>Código: F-DE-PE05-04 Versión: 05</p> | <p>COMUNICACION INTERNA</p> | <p>Página 94 de 95</p> |

INDICADOR11

| | | | |
|--|-------------|-----------------------------|---|
| Implementación de política de almacenamiento de información | | | |
| IDENTIFICADOR | Indicador11 | | |
| DEFINICIÓN | | | |
| Se debe establecer la política de respaldo de la información de toda la información esencial del negocio y del software. | | | |
| OBJETIVO | | | |
| Identificar que se haya implementado la política de almacenamiento de información | | | |
| TIPO DE INDICADOR | | MEDIDA DEL INDICADOR | |
| Operativo | | Política implementada | |
| DESCRIPCION DE VARIABLES | | FORMULA | |
| ¿La entidad cuenta con una política de almacenamiento de información? | | SI=1 NO=0 | |
| METAS | | | |
| CUMPLE | 1 | NO CUMPLE | 0 |

Fuente. Elaboración propia basada en la Guía de Indicadores de gestión para la seguridad de la información (MinTIC, 2015) y en ISO/IEC 27002:2005 (ICONTEC, 2011).

INDICADOR12

| | | | | | |
|---|-------------|----------------------|-----------------------------|----------------------|------|
| Restricciones establecidas | | | | | |
| IDENTIFICADOR | Indicador12 | | | | |
| DEFINICIÓN | | | | | |
| Se debe establecer las restricciones para la instalación de software por parte de los usuarios. | | | | | |
| OBJETIVO | | | | | |
| Busca identificar el grado de avance en la implementación de las restricciones. | | | | | |
| TIPO DE INDICADOR | | | MEDIDA DEL INDICADOR | | |
| Operativo | | | Porcentaje | | |
| DESCRIPCION DE VARIABLES | | | FORMULA | | |
| V15: Número de restricciones Implementadas V16: Número de restricciones que se planearon implementar | | | V15/V16*100 | | |
| METAS | | | | | |
| MINIMA | 80% | SATISFACTORIA | 90% | SOBRESALIENTE | 100% |

Fuente. Elaboración propia basada en la Guía de Indicadores de gestión para la seguridad de la información (MinTIC, 2015) y en ISO/IEC 27002:2005 (ICONTEC, 2011).

