# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

# HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E.

# 2022



**CALLE 22 No. 7 - 93 Parque Bolivar - San Juan de Pasto / Nariño**
Conmutador **7333400** * Fax **7333408 y 7333409**
**www.hosdenar.gov.co** *mail: **hudn@hosdenar.gov.co**

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E.

ACREDITACION EN SALUD

Juntos por la excelencia

**TABLA DE CONTENIDO**

## INDICE DE TABLAS

# 1. INTRODUCCIÓN

Toda información que maneja una entidad pública es muy importante para la relación con el ciudadano, por lo tanto, el resguardo de todo tipo de información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de una Entidad.

Teniendo en cuenta lo anterior dentro del Modelo de Seguridad y Privacidad de la información (MSPI), la Gestión de riesgos se convierte en un tema decisivo y por otra parte se tiene la metodología presentada en la "Guía para la administración del riesgos y el diseño de controles en entidades públicas" del DAFP, buscando que haya una integración y de este modo aprovechar el trabajo adelantado en la identificación de Riesgos para ser complementados con los Riesgos de Seguridad y Privacidad de la Información.

Es importante resaltar que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación de la Confidencialidad, Integridad y Disponibilidad.


CALLE 22 No. 7 - 93 Parque Bolivar - San Juan de Pasto / Nariño
Conmutador 7333400 * Fax 7333408 y 7333409
www.hosdenar.gov.co *mail: hudn@hosdenar.gov.co

# 1. OBJETIVO

Establecer de manera interna un reglamento que permita identificar, medir, controlar, monitorear y comunicar toda clase de riesgos relacionados con la seguridad y privacidad de la información y que de alguna manera interfieren en el cumplimiento de los objetivos estratégicos.

# 2. PROCEDIMIENTO PARA LA GESTION DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Con lo relacionado al procedimiento para la gestión de riesgos asociados a la seguridad y privacidad de la información, la organización ha adelantado estos pasos y ha logrado establecer dicho procedimiento el cual se encuentra aprobado por el SIG con el código PRGES-011 en su última versión del 26 de Octubre de 2018 el cual se encuentra vigente y tiene como objetivo "Establecer la metodología para la gestión integral de los riesgos del HUDN, en cuanto a su identificación, análisis, valoración y tratamiento y para la identificación de las oportunidades de los Sistemas de Gestión". Dentro de dicho procedimiento se ha establecido como alcance el siguiente "Aplica para la gestión de riesgos y oportunidades del SGC, SGSST, SST y SGA, y para la gestión de riesgos de Seguridad de la Información y de Anticorrupción en todos los procesos del HUDN".

Como podemos mirar el procedimiento establecido y vigente abarca los riesgos asociados a la Seguridad y privacidad de la información.

# 3. MATRIZ DE RIESGOS INSTITUCIONAL

La organización ha establecido un procedimiento para la gestión integral del riesgo y como producto de su aplicación ha elaborado la matriz de riesgos institucional, la cual se encuentra identificada dentro del SIG con el código FRGES-014, con fecha de aprobación igualmente del

26 de octubre de 2018 y que se encuentra vigente. La matriz FRGES-014 muestra el consolidado de los riesgos del proceso de Gestión de Información, clasificados así:

**Tabla 1: Riesgos de Proceso**

| |
|---|
| Subregistros asistenciales y administrativos |
| Bajo uso del software in house desarrollado |
| No disponibilidad de Servicios T.I |
| Perdida de la información |
| Usuarios insatisfechos en el servicio de soporte técnico de la mesa de ayuda |
| Software desarrollado desalineado al proceso |
| No disponibilidad de capital para invertir en recursos de T.I |
| Uso de software pirata |
| Desalineación del PETI con la estrategia |
| Falla tecnológica y de redes |
| Pérdida total o parcial de Historias clínicas y documentación |
| Inapropiado almacenamiento y custodia de historias clínicas y documentación |

**Tabla 2: Riesgos Anticorrupción**

| |
|---|
| Pliegos de condiciones hechos a la medida |
| Tráfico de influencias |
| Designar supervisores que no cuentan con conocimientos suficientes para desempeñar la función |

**Tabla 3: Riesgos de sistemas de información**

| |
|---|
| Daño por agua o polvo en servidor de cuarto de Urgencias |
| Colapso estructural por movimiento sísmico que pueda causar daño en los servidores |
| Espionaje remoto de bases de datos de historias clínicas y financiera |
| Hurto de servidores en finanzas y sistemas cuarto piso |
| Hurto de servidores primero, cuarto y quinto |
| Pérdida de información vital para la operación del negocio |
| Incumplimiento en la disponibilidad del personal de soporte |

**Tabla 4: Riesgos de seguridad y salud en el trabajo**

| |
|---|
| Trabajo en Espacios confinados en cuarto de comunicaciones y cielo falso |
| Posturas prolongadas sedentes |
| Movimientos repetitivos |
| Riesgo eléctrico (baja tensión) |
| Mecánico |
| Manejo de cargas livianas: Hombres: <ó=25kg y Mujeres: <ó= 12.5kg |
| Ejecución de actividades con posibilidad de ser golpeado, atrapado por objetos que caen o en movimiento |
| Utilizar herramientas corto punzantes |
| Exposición sustancias químicas no peligrosas. |
| Presencia de microorganismos en el ambiente laboral |
| Falta de Iluminación |

Para un total de 33 Riesgos identificados para el proceso de Gestión de Información.

Para efectos del presente Plan de Tratamiento de Riesgos tomamos los siete (7) riesgos de sistemas de información y haciendo énfasis en los riesgos que tienen calificación consolidada superior a 12, es decir que en el mapa de calor se encuentren en naranja y rojo, producto de este estudio da como resultado la siguiente matriz de riesgos.

## Tabla 5: Matriz de Riesgos Institucional

| PROCESO | GESTIÓN DE LA INFORMACIÓN | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| OBJETIVO DEL PROCESO | Implementar nuevos modelos de gestión de la tecnología, la información y las comunicaciones con base en herramientas que permitan mejorar los aspectos misionales y estratégicos de la Organización. | | | | | | | | | | | | |
| SUBPROCESO SERVICIO | RIESGO | CLASIFICACIÓN | CAUSAS | CONSECUENCIAS | CONTROLES ACTUALES | P | C | NR | NR | NUEVOS CONTROLES PROPUESTOS | RESPONSABLE | PLAZO | INDICADOR | SEGUIMIENTO |
| Todas las áreas | Sistemas de información suceptibles de manipulación y adulteración | Seguridad de la información | 1. Revelar y compartir contraseñas<br>2. Contraseñas debiles | 1.Acceso no autorizado a los sistemas<br>2. Manipulacion y adulteración de información<br>3. Pérdida de la información<br>4. Filtración de información a terceros que puede ser usada en contra del hospital. | 1. Procedimiento para asignar usuarios y contraseñas<br>2. Políticas de control de acceso | 2 | 5 | 10 | RIESGO ALTO | 1. Aplicar políticas de seguridad de la información.<br>2. Despliegue y educación en seguridad de la información | Prof Esp. Gestión de la Información<br><br>Prof. Contratista Gestión de la Información | Frecuente | Número de funcionarios capacitados en seguridad de la información | Gestión de la información - Oficina Control Interno de Gestión |
| Sistemas | Accidentes de alto riesgo con descargas electricas a servidores. | Seguridad de la información | 1. Destinación presupuestal<br>2. Mala ubicación del centro de datos y cableado de red.<br>3. Mala adecuación de pisos en el centro de datos. | 1. Pérdida total de la información<br>2. Perdidas financieras | 1. Acceso restringido al datacenter<br>2. Plan de contingencia de sistemas | 3 | 4 | 12 | RIESGO ALTO | 1. Controles fuertes de acceso físico<br>2. Adecuación y reubicación de datacenter<br>3. Adquisición de nueva tecnología en alta disponibilidad y redundancia<br>4. Actualización del plan de contingencia de sistemas | Prof Esp. Gestión de la Información | 2020 | Controles de acceso implementados<br><br>Datacenter reubicado<br><br>Plan de contingencia actualizado y operativo | Gestión de la información - Oficina Control Interno de Gestión |
| Sistemas | Fenómenos volcánicos | Seguridad de la información | 1. Cercanía a Volcán Galeras<br>2. Fallas geológicas | 1. Pérdida total de la información<br>2. Perdidas financieras | 1. Plan de contingencia de sistemas | 2 | 5 | 10 | RIESGO ALTO | 1. Adquisición de nueva tecnología en alta disponibilidad y redundancia<br>2. Actualización del plan de contingencia de sistemas | Prof Esp. Gestión de la Información | 2020 | % de disponibilidad de los sistemas Gestión para conseguir recursos necesarios<br><br>Plan de contingencia actualizado y operativo | Gestión de la información - Oficina Control Interno de Gestión |
| Todas las áreas | Mal funcionamiento de software y/o hardware | Seguridad de la información | 1. Mal uso de los programas<br>2. Error en las actualizaciones,<br>3. Desactualización de software<br>4. Equipos obsoletos | 1. Daño en el sistema operativo y aplicaciones<br>2. Retraso en las tareas | 1. 2 rondas de mantenimiento preventivo de equipos por año<br>2. Servicio 24/7 de soporte técnico<br>3. Actualización de software | 3 | 2 | 6 | RIESGO MEDIO | 1. Informe de mantenimientos<br>2. Informe de actualización de equipos y relación de números de equipos nuevos en cada servicio. | Prof Esp. Gestión de la Información<br>Tecnico Operativo Gestión de la Información | Frecuente | N/A | Gestión de la información - Oficina Control Interno de Gestión |

| SUBPROCESO SERVICIO | RIESGO | CLASIFICACIÓN | CAUSAS | CONSECUENCIAS | CONTROLES ACTUALES | P | C | NR | NR | NUEVOS CONTROLES PROPUESTOS | RESPONSABLE | PLAZO | INDICADOR | SEGUIMIENTO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Sistemas | Saturación del sistema de información, mal funcionamiento del equipo | Seguridad de la información | 1. Alto volumen de consultas<br>2. Multiples sesiones en el mismo equipo | 1. Bloqueo del sistema de información | 1. Servicio 24/7 de soporte técnico | 2 | 3 | 6 | RIESGO MEDIO | Mantener el control | Tecnico Operativo Gestión de la Información Técnicos 24/7 | Frecuente | N/A | Gestión de la información - Oficina Control Interno de Gestión |
| Sistemas | Incumplimiento en el mantenimiento del sistema de información | Seguridad de la información | 1. Proveedor no entrega a tiempo y verificadas las actualizaciones solicitadas por el HUDN | 1. Mal funcionamiento del sistema de información<br>2. Incumplimiento de normas | 1. Realizar pruebas y verificación de actualizaciones del sistema de información | 2 | 2 | 4 | RIESGO BAJO | Mantener el control | Coordinador Desarrollo de software y BD Profesional Universitario Area Financiera Facturación Central | Cuando se realice solicitud de ajuste del sistema | N/A | Gestión de la información - Oficina Control Interno de Gestión |
| Todas las Áreas | Perdida de suministro de energia | Seguridad de la información | 1. Fallas en conexión eléctrica institucional<br>2. Fallas externas | 1. Pérdida de registros del usuario<br>2. Inoportunidad en la atención<br>3. Perdida de continuidad en la prestación del servicio | Uso de sistema de soporte para abastecimiento de energía | 3 | 4 | 12 | RIESGO ALTO | 1, Que los equipos de computo esten soportados y conectados a la red electrica regulada.<br>2. Instalacion de tomas de patas trabadas. y plantas electricas.<br>3.Verificación de las áreas afectadas por falta de UPS | R. fisicos Profesional de tecnología de la información | Según Evento | Gestión para conseguir recursos necesarios | Gestión de la información - Oficina Control Interno de Gestión |
| Todas las Áreas | Posibles errores en el uso del aplicativo Dinamica | Seguridad de la información | 1. Sistema de información no intuitivo | 1. Perdida de confiabilidad en la información del sistema de información | 1. Se cuenta con contrato de soporte y mejoras al sistema con el proveedor | 3 | 4 | 12 | RIESGO ALTO | 1. Revisión mensual del sistema de informacion para realizar ajustes<br>2. Control estricto a las nuevas utilidades incluidas en las actualizaciones | Profesional de tecnología de la información Coordinador Desarrollo de software y BD Soporte Técnologico | Frecuente | Solicitudes de mejora implementadas / Solicitudes de mejora realizadas al proveedor | Gestión de la información - Oficina Control Interno de Gestión |

| SUBPROCESO SERVICIO | RIESGO | CLASIFICACIÓN | CAUSAS | CONSECUENCIAS | CONTROLES ACTUALES | P | C | NR | NR | NUEVOS CONTROLES PROPUESTOS | RESPONSABLE | PLAZO | INDICADOR | SEGUIMIENTO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Gestión Financiera / Contabilidad | Ingresos de datos falsos o corruptos | Seguridad de la Información | 1. Falta de control de permisos y perfiles de usuarios del sistema DGH. | 1. Informacion errada, manipulada o adulterada. | 1. Asignacion de permisos de acuerdo al ususrio por el area de sistemas. | 2 | 4 | 8 | RIESGO MEDIO | Mantener el control | Profesional Universitario Tecnología de la Información | Frecuente | N/A | Gestión de la información - Oficina Control Interno de Gestión |
| Todas las áreas | Pérdida de la información | Seguridad de la Información | 1. Omisión en la responsabilidad de crear copias de seguridad al sistema de información. | 1. Perdida de la información | 1. Designación de la función de realizar las copias periodicamente desde el área de sistemas. | 2 | 4 | 8 | RIESGO MEDIO | Adquisición y montaje de nuevos servidores, montaje de Cluster de backups y licenciamiento para copias en la Nube. | Prof Esp. Gestión de la Información | 2020 | N/A | Gestión de la información - Oficina Control Interno de Gestión |
| Gestión Financiera / Costos | Mal funcionamiento del sistema de informacion | Seguridad de la Información | 1. Deficiencia en procedimientos de seguridad de la información<br>2. Deficiente cobertura a red de internet en áreas en donde se requiere para cumplir con la misión operativa de la organizacion.<br>3. Deficiente capacidad de número de equipos para el procesamiento de la información | 1. Afecta negativamente en la prestacion del servicio.<br>2. Información inoportuna a clientes internos y externos. | 1. Mesa de ayuda<br>2. Análisis de causas de las dificultades presentadas frente a lo esperado. | 4 | 3 | 12 | RIESGO ALTO | 1. Actualizaciones continuas del sistema de información.<br>2. Planes de contingencia para prevenir eventos adversos relacionados con la informacion.<br>3. Estudios y verificación en que áreas se requiere ampliación de acceso a redes de internet | Prof Esp. Gestión de la Información | 2020 | Solicitudes de mejora implementadas / Solicitudes de mejora hechas al proveedor | Gestión de la información - Oficina Control Interno de Gestión |
| Gestión Financiera / Costos | Información errónea | Seguridad de la Información | 1. Frecuente movilidad de personal ocasionando una gestión no cofiable en el registro de la información. | 1. Información con margen de error | 1. Inducción a nuevos funcionarios | 4 | 4 | 16 | RIESGO MUY ALTO | 1. Capacitación a usuarios responsables del registro de información<br>2. Validación de fuentes de información | Prof Esp. Gestión de la Información Profesional Universitario Tecnología de la Información | 2020 | Usuarios capacitados en el manejo del sistema / Usuarios con clave de acceso asignada | Gestión de la información - Oficina Control Interno de Gestión |

| SUBPROCESO SERVICIO | RIESGO | CLASIFICACIÓN | CAUSAS | CONSECUENCIAS | CONTROLES ACTUALES | P | C | NR | NR | NUEVOS CONTROLES PROPUESTOS | RESPONSABLE | PLAZO | INDICADOR | SEGUIMIENTO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Todas las áreas | Equipos obsoletos | Seguridad de la información | 1. Falta de actualización TICS | 1. Alteración Proceso Docencia Investigación | 1. Adquisición o reposición de equipos de computo | 4 | 3 | 12 | RIESGO ALTO | 1. Acciones para compra de equipos | Prof Esp. Gestión de la Información | 2020 | Equipos comprados / Equipos obsoletos | Gestión de la información - Oficina Control Interno de Gestión |
| Todas las áreas | Virus informático | Seguridad de la información | 1. Antivirus Caducado<br>2. Falta de mantenimiento.<br>3. Desconocimiento del manejo adecuado de los equipos e internet.<br>4. Manejo sin previsión de los medios magnéticos. | 1. Fallas en el funcionamiento de los equipos de cómputo cuando sea el caso.<br>2. Pérdida de documentos o información importante. | 1. Asistencia de los técnicos de la oficina de sistemas.<br>2. 2 rondas de mantenimiento preventivo de equipos por año<br>Servicio 24/7 de soporte técnico | 2 | 3 | 6 | RIESGO MEDIO | 1. Realizar capacitaciones periódicas para el buen uso de los equipos.<br>2. Mantenimiento periódico de los equipos.<br>3. Plan de adquisición y licenciamiento de antivirus en la Nube. | Prof Esp. Gestión de la Información<br>Profesional Universitario Tecnología de la Información | Frecuente | Oportunidad en la atención de incidentes | Gestión de la información - Oficina Control Interno de Gestión |
| Todas las áreas | Destrucción del equipo de computo o los medios de almacenamiento | Seguridad de la información | 1. Mala práctica de trabajo.<br>2. Manejo no autorizado de medios de almacenamiento (USB, Discos externos, etc). | 1. Pérdida de la información.<br>2, Fallas en funcionamiento de los equipos de computo. | 1. Asistencia de los técnicos de la oficina de sistemas. | 2 | 4 | 8 | RIESGO MEDIO | 1. Realizar capacitaciones periódicas para el buen uso de los equipos.<br>2. Mantenimiento periódico de los equipos. | Prof Esp. Gestión de la Información<br>Tecnico Operativo Gestión de la Información | 2020 | Porcentaje de Cumplimiento del Cronograma de Mantenimiento Preventivo | Gestión de la información - Oficina Control Interno de Gestión |
| Todas las áreas | Corrupción de datos | Seguridad de la información | 1. Información variable en los datos recolectados, diferentes fuentes de información | 1. Reprocesos y retrasos en los procedimientos | PRSGI - 009 IDENTIFICACION, CONSOLIDACION Y DISPOSICION DE INFORMACION | 3 | 2 | 6 | RIESGO MEDIO | Mantener el control | Profesional Especializado de Gestión de Información<br>Profesional de Planeación de TI<br>Profesional de Planeación<br>Técnico Administrativo - Estadística<br>Líderes de los procesos | Frecuente | Porcentaje de Cumplimiento del Cronograma de Copias de Seguridad | Gestión de la información - Oficina Control Interno de Gestión |

| SUBPROCESO SERVICIO | RIESGO | CLASIFICACIÓN | CAUSAS | CONSECUENCIAS | CONTROLES ACTUALES | P | C | NR | NR | NUEVOS CONTROLES PROPUESTOS | RESPONSABLE | PLAZO | INDICADOR | SEGUIMIENTO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Gestión Financiera / Facturación | Saturación del sistema de información | Seguridad de la Información | 1. Bajo nivel de almacenamiento | 1. Perdida de información | 1. Solicitud a sistemas y Gerencia sobre la ampliación de la capacidad de almacenamiento de la información en la nube, con la adquisición de un servidor exclusivo para facturación y asi prevenir inconvenientes futuros. | 2 | 3 | 6 | RIESGO MEDIO | Adquisición y montaje de nuevos servidores | Prof Esp. Gestión de la Información<br>Tecnico Operativo Gestión de la Información | 30-04-2020 | Compra del servidor | Gestión de la información - Oficina Control Interno de Gestión |
| Gestión Financiera / Tesorería | Piratería | Seguridad de la Información | Robo o cesión de claves | Secuestro o robo de información | 1. Control de caducidad de la contraseña de los aplicativos. | 4 | 4 | 16 | RIESGO MUY ALTO | 1. Crear el Protocolo de seguridad informática? | Ofi. Financiera<br>Prof Esp. Gestión de la Información | 2020 | Capacitaciones realizadas / Capacitaciones programadas | Gestión de la información - Oficina Control Interno de Gestión |
| Todas las áreas | Daño físico - daño por agua | Seguridad de la información | 1. Inundaciones<br>2. Ruptura de tuberias.<br>3. Canales en mal estado y antiguos | 1. Perdida de informaciòn<br>2. Daño de equipos | 1. Mantenimiento preventivo de infraestructura | 1 | 4 | 4 | RIESGO BAJO | 1. Informe de reporte de eventos relacionados y análisis de cada uno de elllos. | Arquitecto<br>Prof Esp. Gestión de la Información | Frecuente | Porcentaje de Cumplimiento del Cronograma de Mantenimiento Preventivo | Gestión de la información - Oficina Control Interno de Gestión |
| Todas las áreas | Falsificación de derechos en la prestacion de servicios a los usuarios | Seguridad de la información | 1. No disponibilidad de recursos.<br>2. Falta de comprobacion de derechos de usuarios.<br>3. Falta de actualizacion de bases de datos.<br>4. Ingreso en admisiones con datos por personas que no conocen al usuario, error en digitación de datos, no corroborar frente al paciente los datos de registro y admisión por el médico | 1. Sanciones<br>2. Demandas | 1. Existe un rubro general de mantenimiento, desde donde se destinan recursos para insumos y mantenimientos correctivos y adquisición de tecnología. | 5 | 4 | 20 | RIESGO MUY ALTO | 1. Establecer dentro del presupuesto un rubro específico para la gestion de TI | Gestion de información Subgerencia Administrativa y financiera | 2020 | Proceso de Gestión de Información con presupuesto específico asignado | Gestión de la información - Oficina Control Interno de Gestión |

| SUBPROCESO SERVICIO | RIESGO | CLASIFICACIÓN | CAUSAS | CONSECUENCIAS | CONTROLES ACTUALES | P | C | NR | NR | NUEVOS CONTROLES PROPUESTOS | RESPONSABLE | PLAZO | INDICADOR | SEGUIMIENTO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Todas las áreas | Saturación del sistema de información | Seguridad de la información | 1. Software desarrollado desalineado al proceso.<br>2. Desarrollo con alcance insuficiente<br>3. Requerimientos e insumos levantados de manera incompleta | 1. Insatisfacción de usuarios con el software desarrollado.<br>2. Perdida de credibilidad en el proceso<br>3. Retrazos en la prestación del servicio | 1. Realización dos rondas de mantenimiento preventivo de equipos al año.<br>2. Monitoreo del funcionamiento de servidores constante. | 4 | 2 | 8 | RIESGO MEDIO | 1. Contar con unidades para quemar información de BackUp<br>2. Contratar el servicio de custodia externa de la información por lo menos de la última copia de cada mes<br>3. Crear el procedimiento para la custodia externa | Prof Esp. Gestión de la Información | 1 y 2 Frecuente<br>3. 2020 | 1. Cantidad de equipos de backups<br>2. Servicio de custodia de información contratado<br>3. Procedimiento de custodia externa establecido | Gestión de la información - Oficina Control Interno de Gestión |
| Todas las áreas | Manipulacion con Software | Seguridad de la información | 1. Divulgación de claves.<br>2. Permisos de consulta a múltiples perfiles | 1. Inoportunidad en la prestación del servicio.<br>2. Pérdida de integridad de la información.<br>3. Bloqueo de usuarios en la HCD<br>4. Reprocesos<br>5. Glosas | 1. Se cuenta con equipos de seguridad perimetral de marca<br>2. Antivirus licenciado<br>3. Control de acceso con chapa de seguridad | 2 | 2 | 4 | RIESGO BAJO | 1. Control de acceso con dispositivo biométrico<br>2. Acceso solo a personal autorizado<br>3. Independizar el acceso a la oficina de sistemas | Prof Esp. Gestión de la Información | 1 y 2 Frecuente<br>3. (debe tener un plazo) | 1. Porcentaje de dispositivos biométricos instalados<br>2. Acceso a la oficina de sistemas independizado | Gestión de la información - Oficina Control Interno de Gestión |
| Todas las áreas | Hurto y daño de equipos | Seguridad de la información | 1. Falta de apropiación del personal para el cuidado de los equipos | 1. Perdida del patrimonio del hospital<br>2. Retraso en el trabajo<br>3. Perdida de información | 1 Camaras de seguridad y vigilancia. | 1 | 3 | 3 | RIESGO BAJO | 1. Implementación de medidas de seguridad y detectores<br>2. copias de seguridad y equipos de backup | Prof Esp. Gestión de la Información<br>Personal asistencial | 1. inmediato<br>2. Permanente | Eqipos dados de baja | Gestión de la información - Oficina Control Interno de Gestión |
| Todas las áreas | Destrucción del equipo de computo o de los medios | Seguridad de la información | 1. Por caida involuntaria del equipo<br>2. Emergencias naturales y antrópicas | 1. Posible perdida de información del proceso | 1. Plan de contingencia de sistemas | 2 | 3 | 6 | RIESGO MEDIO | 1. Actualización de tecnología y asegurar equipos a módulos de transporte | Coordinador del servicio<br>Prof Esp. Gestión de la Información<br>Personal asistencial | Frecuente | Porcentaje de Cumplimiento del Cronograma de Mantenimiento Preventivo | Gestión de la información - Oficina Control Interno de Gestión |
| Todas las áreas | Intrusión en la privacidad personal | Seguridad de la información | 1. No guardar reserva de los usuarios con eventos de notificación en salud pública | Mal uso de información relevante | Entregar información unicamente a los entes de control y responsables del aseguramiento para garantizar la continuidad de su tratamiento | 2 | 2 | 4 | RIESGO BAJO | 1. Depuracion de la información.<br>2. Control de entrega de informacion a entes internos y externos. | Vigilancia Epidemiológica / Prof Esp. Gestión de la Información | Frecuente | Porcentaje de adopción de políticas de TI | Gestión de la información - Oficina Control Interno de Gestión |

HOSPITAL UNIVERSITARIO
DEPARTAMENTAL DE NARIÑO E.S.E.

ACREDITACION EN SALUD

**¡Trabajamos por mi Nariño,**
**tu salud,**
**nuestro compromiso!**

***CALLE 22 No. 7 - 93 Parque Bolivar - San Juan de Pasto / Nariño***
*Conmutador* ***7333400*** ** Fax* ***7333408 y 7333409***
***www.hosdenar.gov.co*** **mail:* ***hudn@hosdenar.gov.co***

icontec ISO 9001 icontec ISO 14001 icontec ISO 45001

CERTIFIED IQNet MANAGEMENT SYSTEM

## 5. INDICADORES

Como se observa en la tabla anterior por cada riesgo y por cada control propuesto se han fijado indicadores individuales, pero a nivel general es pertinente establecer un indicador que agrupe todas las actividades el cual quedaría de la siguiente manera y sirve para medir la eficacia en la ejecución del plan:

$$ICA = \frac{\text{No. de Actividades cumplidas}}{\text{No. de actividades programadas}} * 100$$

Donde ICA es el Índice de Cumplimiento de Actividades

## 6. EJECUCIÓN

La ejecución consiste en llevar a cabo la implementación de los controles propuestos en el cuadro anterior, procurando que se realicen dentro de los tiempos establecidos y sean desarrolladas por los responsables asignados.

Para poder llevar a cabo con éxito la ejecución es importante recalcar el compromiso de la Alta y Media dirección para asignar los recursos económicos necesarios a las actividades que así lo requieran.

## 7. MONITOREO

Le corresponde a la organización y a cada una de las tres líneas de defensa que establece MIPG hacer un seguimiento al presente plan para determinar su efectividad, para lo cual debe realizar las siguientes actividades:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.

Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.

- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

## 8. MEJORAMIENTO CONTINUO

Es responsabilidad de la organización dar garantía para la mejora continua en la gestión de riesgos en este caso de los asociados a la seguridad y privacidad de la información, teniendo en cuenta lo anterior se debe fijar que cuando haya hallazgos, falencias o incidentes de seguridad y privacidad de la información se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos, por otra parte es importante que la organización establezca y haga frente a las consecuencias que se derivan de lo que llegó a materializarse.

Deben definirse las acciones para mejorar continuamente la gestión de riesgos de seguridad y privacidad de la información de la siguiente manera:

- Revisar y evaluar los hallazgos encontrados en los informes de los entes de control.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado,

así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad o de los servicios que presta al ciudadano.

- Adicionalmente, se sugiere llevar un registro documentado del tratamiento realizado al hallazgo, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuros hallazgos.

Realizo

ROBERTO EDUARDO FREIRE BURBANO
Ing. Sistemas Esp.
HUDN - 2022

Reviso

HENRY LUIS RODRIGUEZ CARDENAS
Coordinador Gestión de Información

HOSPITAL UNIVERSITARIO
DEPARTAMENTAL DE NARIÑO E.S.E.

ACREDITACION EN SALUD

**¡Trabajamos por mi Nariño,
tu salud,
nuestro compromiso!**

***CALLE 22 No. 7 - 93 Parque Bolivar - San Juan de Pasto / Nariño***
*Conmutador* ***7333400*** * *Fax* ***7333408 y 7333409***
***www.hosdenar.gov.co*** **mail:* ***hudn@hosdenar.gov.co***

icontec ISO 9001 icontec ISO 14001 icontec ISO 45001

CERTIFIED IQNet MANAGEMENT SYSTEM