**Establecer políticas y procedimientos para controlar los riesgos**

Luego de haber realizado el respectivo análisis de riesgos e identificado los controles, se diseña el documento de “Declaración de Aplicabilidad” en la cual se hizo una revisión de los 96 controles que propone la ISO/IEC 27002 y a base de criterios se determinó la aplicabilidad de cada uno de ellos a la organización. Es exigido por la ISO/IEC 27001 ya que permite asegurar que no se está omitiendo algún control y si algún control no aplicase a la empresa, se realiza la justificación. El diseño del documento se puede ver en la siguiente tabla

|  |  |
| --- | --- |
| Campo | Descripción |
| Sección | Número de Cláusula referenciada de la ISO/IEC 27001 |
| Objetivo | Objetivo de la cláusula |
| Control | Descripción del control |
| Aplicación | SI: Si es aplicable a la empresa, No: Si no es aplicable a la empresa |
| Justificación de Exclusión | Justificación porque se está excluyendo el control |
| Justificación de Inclusión | Criterios para la selección de controles: LR: Requemamientos Legales, CO: Obligaciones Contractuales, BR/BP: Requerimientos del negocio/Mejores Prácticas, RRA: Resultado de Análisis de Riesgos |
| Adaptación | Descripción de cómo se aplicaría el control |

Se elabora la declaración de aplicabilidad según los campos especificados:

**Declaración de aplicabilidad**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sec. | Objetivo | Control | Justificación de exclusión | Justificación Inclusión | | | | Aplicación | Adopción |
| LR | CO | BR/BP | RRA | Si/No |
| 5 | Políticas de seguridad de la información | | | | | | | | |
| 5,1 | Directrices establecidas por la dirección para la seguridad de la información | | | | | | | | |
| 5.1.1 | Políticas para la seguridad de la información | Existen políticas de seguridad de la información pero no han sido documentadas, se debe redactar un documento que políticas para que sea distribuido y conocido por todo el personal incluido en el proceso del SGSI |  |  |  | X |  | Si | Se diseñó e implementó el documento de Política de Seguridad de la Información. **Control C001.** |
| 5.1.2 | Revisión de las políticas para seguridad de la información | Se debe establecer un procedimiento que permita la revisión periódica de las políticas de la seguridad de la información por lo menos cada año |  |  |  | X |  | Si | Se diseñó e implementó el documento de Política de Seguridad de la Información, en el cual se determina el periodo de revisión de la política. **Control C002.** |
| 6 | Organización de la seguridad de la información | | | | | | | | |
| 6,1 | Organización interna. | | | | | | | | |
| 6.1.1 | Roles y responsabilidades para la seguridad de información | Se deben definir roles y responsabilidades de acuerdo a las políticas de seguridad de la información a todos los que interactúen con el SGSI |  |  |  | X |  | Si | Se diseñó e implementó el documento de Política de Seguridad de la Información, en el cual se determinan los roles y responsabilidades respecto a la seguridad de la información. **Control C003.** |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sec. | Objetivo | Control | Justificación de exclusión | Justificación Inclusión | | | | Aplicación | Adopción |
| LR | CO | BR/BP | RRA | Si/No |
| 6.1.2 | Separación de deberes | Se deben separar las ares consideradas de gran importancia para que así los deberes y responsabilidades asignadas sean separadas, de esta forma se evita el uso indebido de los activos de la organización |  |  |  | X | X | Si | Los procesos se han determinado considerando segregación en los procesos. **Control C004.** |
| 6.1.3 | Contacto con las autoridades | En el documento de políticas de la seguridad de la información se debe contemplar un procedimiento que permita gestionar el contacto permanente con autoridades reguladoras de seguridad de la información | La organización no tiene contacto con autoridades reguladoras de los procesos de negocio. |  |  |  |  | No |  |
| 6.1.4 | Contacto con grupos de interés especial | Es importante que la persona encargada de la seguridad informática gestione el contacto permanente con grupos de interés, estos pueden ser foros, chats, wiki, comunidades relacionadas con la seguridad informática, con la intención de estar actualizados en aspectos relacionados a la seguridad | Las ejecuciones en seguridad de la información no están a cargo de personal operativo de la empresa. |  |  |  |  | No |  |
| 6.1.5 | Seguridad de la información en la gestión de proyectos | La seguridad de la información se debe tratar en cualquier proyecto. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 6,2 | Dispositivos móviles y teletrabajo. | | | | | | | | |
| 6.2.1 | Política para dispositivos móviles | Se deben aplicar políticas para el uso adecuado de dispositivos móviles, su uso inadecuado representa grandes riesgos | Los procesos no tienen participación de dispositivos móviles. |  |  |  |  | No |  |
| 6.2.2 | Teletrabajo | Se deben aplicar políticas para el uso adecuado del acceso remoto por VPN su uso inadecuado representa grandes riesgos |  |  |  |  | X | Si | Se diseñó el documento Acuerdo de Confidencialidad el cual estipula que la información que corresponde a los procesos internos, así como la información de los pacientes atendidos por la mediplus, son de carácter confidencial y la divulgación de estos conlleva castigos penales, así como la ruptura de la relación con la organización. Control C005. |
| 7 | Seguridad de los recursos humanos | | | | | | | | |
| 7,1 | Antes de asumir el empleo. | | | | | | | | |
| 7.1.1 | Selección | Se deben realizar una exhaustiva comprobación de los antecedentes del personal como empleados, contratistas, terceros, con el fin de saber su procedencia, referencias personales, judiciales entre otras | No representa un riesgo crítico para la empresa ya que cuenta con el mismo personal por años. |  |  |  |  | No |  |
| 7.1.2 | Términos y condiciones del empleo | Se debe diseñar un documento que permita a los empleados, contratistas y terceros firmar cláusulas de confidencialidad con la organización, manejo adecuado de recursos tecnológicos |  | X | X |  |  | Si | Se diseñó el documento Acuerdo de Confidencialidad el cual estipula que la información que corresponde a los procesos internos, así como la información de los pacientes atendidos por la mediplus, son de carácter confidencial y la divulgación de estos conlleva castigos penales, así como la ruptura de la relación con la organización. Control C005. |
| 7,2 | Durante la ejecución del empleo. | | | | | | | | |
| 7.2.1 | Responsabilidades de la dirección | Se debe exigir a los empleados, contratistas y terceros el cumplimiento a cabalidad de las políticas de seguridad de la información implementadas por la Cía | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información | Se debe capacitar a todo el personal en aspectos relacionados con la seguridad de la información |  |  |  | X |  | Si | El personal de mediplus es sensibilizado respecto a temas de seguridad de la información. Control C006. |
| 7.2.3 | Proceso disciplinario | Se deben establecer políticas sobre sanciones que se aplicarán a quienes incumplan con lo descrito en las políticas de seguridad |  |  |  | X |  | Si | Se diseñó e implementó el documento de Política de Seguridad de la Información, en el cual se determinan las penalidades sobre el incumplimiento de la política. **Control C007.** |
| 7,3 | Terminación o cambio de empleo | | | | | | | | |
| 7.3.1 | Terminación o cambio de responsabilidades de empleo | Se debe informar a los empleados en los casos donde las responsabilidades y deberes que les fueron asignados durante el empleo, los cobijan aun cuando se realice una terminación o cambio de contrato | No representa un riesgo crítico para la empresa ya que no se realizan cambios de puestos. |  |  |  |  | No |  |
| 8 | Gestión de activos | | | | | | | | |
| 8,1 | Responsabilidad por los activos | | | | | | | | |
| 8.1.1 | Inventario de activos | Se debe contar con un inventario detallado de los activos que posee la Cía |  |  |  | X | X | Si | Se identificó y clasificó los activos de los procesos relevantes de la organización teniendo como resultado el Inventario de Activos de Información. **Control C008.** |
| 8.1.2 | Propiedad de los activos | Además de la implementación del control anterior, se debe identificar en custodia de quien se encuentra actualmente el activo |  |  |  | X | X | Si | El inventario de activos diseñado tiene información actualizada del propietario (responsable) del activo de información. **Control C009.** |
| 8.1.3 | Uso aceptable de los activos | Debe existir una clausula donde los empleados se comprometan a realizar un uso aceptable de los activos de la organización |  |  |  | X |  | Si | Se diseñó e implementó la política específica de Gestión de Activos en la que se establece el uso que los empleados le deben dar a los activos de información. **Control C010.** |
| 8.1.4 | Devolución de activos | Se debe establecer un proceso para la devolución de los activos para cuando los empleados cambien de puesto o cuando se termine su contrato |  |  |  | X |  | Si | Se diseñó e implementó la política específica de Gestión de Accesos en la que se establece el proceso de devolución de activos ante el cese del personal. **Control C011.** |
| 8,2 | Clasificación de la información | | | | | | | | |
| 8.2.1 | Clasificación de la información | Se debe establecer un procedimiento que permita clasificar la información de acuerdo a su valor | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 8.2.2 | Etiquetado de la información | La información debe estar debidamente rotulada, además esta rotulación se debe clasificar de acuerdo al valor que representa la información para la empresa | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 8.2.3 | Manejo de activos | Se debe contar con procedimientos que ayuden en el | Se cubrirá con el control C010. |  |  |  |  | No |  |
|  |  | adecuado manejo que se le debe dar a un activo |  |  |  |  |  |  |  |
| 8.3.1 | Gestión de medios removibles | Se deben establecer políticas sobre el correcto manejo que se le deben dar a los medios removibles, puesto que estos son necesarios en el desarrollo de las labores diarias. |  |  |  | X | X | Si | Se diseñó e implementó la política específica de Gestión de Activos en la que se establece que los medios removibles deben ser inhabilitados en todas las computadoras de la mediplus. Control C012. |
| 8.3.2 | Disposición de los medios | Protección de la información cuando los medios sean destinados a labores diferentes a las actuales, se podría hablar de un procedimiento de eliminación de información en estos casos. | No aplica a la empresa. |  |  |  |  | No |  |
| 8.3.3 | Transferencia de medios físicos | Definir procedimientos que permitan que la información almacenada en estos no sea divulgada, modificada o eliminada. |  | X |  | X | X | Si | Se tiene como regla en el proceso de Procesamiento que el medico ocupacional del cliente puede decepcionar los resultados de los exámenes. **Control C013.** |
| 9 | Control de acceso | | | | | | | | |
| 9,1 | Requisitos del negocio para control de acceso | | | | | | | | |
| 9.1.1 | Política de control de acceso | Establecer políticas que permitan el acceso a la información de acuerdo a privilegios establecidos según sus funciones |  |  |  | X |  | Si | Se diseñó e implementó la Política Específica de Gestión de Accesos. **Control C014.** |
| 9.1.2 | Política sobre el uso de los servicios de red | Definir el acceso a la red para el desarrollo de funciones que les fueron asignadas. | No representa un riesgo crítico para la empresa ya que el acceso a la red no asegura el acceso a las aplicaciones de la mediplus. |  |  |  |  | No |  |
| 9,2 | Gestión de acceso de usuarios | | | | | | | | |
| 9.2.1 | Registro y cancelación del registro de usuarios | Todos los usuarios con acceso a sistema de información deben estar debidamente registrados, adicionalmente se debe dar de baja a los que ya no hagan parte de la organización o no hagan uso del sistema. |  | X | X | X | X | Si | El personal que cesa de la empresa se le debe retirar los accesos a los sistemas de información en un periodo oportuno. **Control C015.** |
| 9.2.2 | Suministro de acceso de usuarios | Implementar un procedimiento que permita a los usuarios del sistema acceder al sistema o negar el acceso a este cuando se considere necesario. |  |  |  | X |  | Si | Los ordenadores deben requerir usuarios y contraseña para el acceder a los mismos. **Control C016.** |
| 9.2.3 | Gestión de derechos de acceso privilegiado | Se deben establecer privilegios de acceso a la información de acuerdo al desempeño de sus funciones. |  |  |  | X |  | Si | Existe una revisión periódica de accesos otorgados en el sistema Mediweb. **Control C017.** |
| 9.2.4 | Gestión de información de autenticación secreta de usuarios | Esta información sólo debe ser accesada por personal con privilegios especiales |  |  |  | X |  | Si | Sólo personal autorizado tiene acceso a la Gestión de Accesos en los sistemas de información. **Control C018.** |
| 9.2.5 | Revisión de los derechos de acceso de usuarios | Monitoreo de privilegios asignados a usuarios con el fin de identificar si los privilegios asignados son adecuados para el desarrollo de sus funciones. |  |  |  | X | X | Si | Se cubrirá con el control **C017**. |
| 9.2.6 | Retiro o ajuste de los derechos de acceso | Se debe dar de baja o modificar los privilegios de acceso a la información en caso de traslado del usuario o retiro de la organización. |  | X |  | X |  | Si | Se cubrirá con el control **C015**. |
| 9,3 | Responsabilidades de los usuarios | | | | | | | | |
| 9.3.1 | Uso de la información de autenticación secreta | Se deben crear perfiles para el acceso a información considerada de suma importancia para la empresa |  |  |  | X | X | Si | Se cubrirá con el control **C018**. |
| 9,4 | Control de acceso a sistemas y aplicaciones | | | | | | | | |
| 9.4.1 | Restricción de acceso Información | Restringir el acceso a la información por parte de personal no autorizado. |  | X | X | X | X | Si | Los activos físicos críticos se encuentran en un ambiente restringido al público. **Control C019.** |
| 9.4.2 | Procedimiento de ingreso seguro | Se deben establecer procedimientos que restrinjan el acceso a la información a personal no autorizado |  | X | X | X |  | Si | Se cubrirá con el control **C016**. |
| 9.4.3 | Sistema de gestión de contraseñas | Se deben establece políticas de gestión de contraseñas como caducidad, bloqueo después de determinado número de intentos, parámetros para creación de contraseñas seguras. |  |  |  | X | X | Si | Los sistemas de información han sido configurados con la política de contraseña definida por la organización. **Control C020.** |
| 9.4.4 | Uso de programas utilitarios privilegiados | Restringir el uso de programas utilitarios ya que pueden violentar la seguridad de las contraseñas, pues algunos revelan las contraseñas, vulnerando la seguridad. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 9.4.5 | Control de acceso a códigos fuente de programas | Políticas de acceso al código fuente, este sólo debe ser accesado por el personal autorizado | No aplica a la empresa. |  |  |  |  | No |  |
| 10 | Criptografía | | | | | | | | |
| 10,1 | Controles criptográficos | | | | | | | | |
| 10.1.1 | Política sobre el uso de controles criptográficos | Se deben establecer controles criptográficos que permitan la confidencialidad, disponibilidad, integridad y no repudio de la información | Se establecerán controles de criptografía fuera de una política. |  |  |  |  | No |  |
| 10.1.2 | Gestión de llaves | Se deben establecer controles criptográficos que permitan la confidencialidad, disponibilidad, integridad y no repudio de la información |  | X |  | X |  | Si | Las tablas de información confidencial son encriptados a nivel de base de datos. **Control C021.** |
| 11 | Seguridad física y del entorno | | | | | | | | |
| 11,1 | Áreas seguras | | | | | | | | |
| 11.1.1 | Perímetro de seguridad física | Se debe establecer un perímetro de tal forma que los sitios donde se encuentren los activos tengan accesos restringido |  | X | X | X | X | Si | Se cubrirá con el control **C019.** |
| 11.1.2 | Controles físicos de entrada | Se debe restringir el acceso a sitios seguros como centro de cableado, ubicación del servidor, espacios donde se encuentre información confidencial, estos sitios deben permanecer con llave. |  | X | X | X | X | Si | El centro de datos se encuentra con acceso restringido a personal autorizado. **Control C022.** |
| 11.1.3 | Seguridad de oficinas, recintos e instalaciones | Restringir el acceso a personal no autorizado, las áreas deben estar demarcadas dando aviso que son sitios restringidos |  | X | X | X |  | Si | En la mediplus las áreas restringidas están señalizadas. Control C023. |
| 11.1.4 | Protección contra amenazas externas y ambientales | Se debe contar con detectores de humo y humedad, ubicación de extinguidores en sitios estratégicos, cuartos técnicos con aire acondicionado, adquisición de pólizas contra robo y desastres naturales |  |  |  | X | X | Si | En la mediplus se han implementado medidas de seguridad ante amenazas internas como extintores, alarmas, luminarias ante falta de electricidad, etc. Control C024. |
| 11.1.5 | Trabajo en áreas seguras | Se deben preservar los sitios donde se encuentren activos valiosos con el fin de protegerlos contra daños intencionados | Se cubrirá con el control C013. |  |  |  |  | No |  |
| 11.1.6 | Áreas de despacho y carga | Se deben designar sitios especiales para carga y despacho, lo recomendable es que estén aislados de los denominados sitios seguros o restringidos | No aplica a la empresa. |  |  |  |  | No |  |
| 11,2 | Equipos | | | | | | | | |
| 11.2.1 | Ubicación y protección de los equipos | Los equipos deben estar ubicados en sitios seguros, de esta forma se protegen contra robo, accesos no autorizados. |  | X | X | X |  | Si | Se cubrirá con el control **C022.** |
| 11.2.2 | Servicios de suministro | Se debe contar con un adecuado suministro y respaldo de energía | Se cuentan con procedimientos de continuidad de negocio. |  |  |  |  | No |  |
| 11.2.3 | Seguridad del cableado | Se debe proteger el cableado eléctrico y de datos de posibles daños como interceptaciones con el fin de causar daño. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 11.2.4 | Mantenimiento de equipos | Se debe contar con mantenimiento preventivo y correctivo en períodos de tiempo establecidos, con el fin de evitar daños en hardware, actualización de software. |  |  |  | X |  | Si | Los activos de hardware y software deben tener un mantenimiento anual. **Control C025.** |
| 11.2.5 | Retiro de activos | Se debe definir un procedimiento que autorice el retiro de activos de la empresa tales como equipos de cómputo, software. | No aplica a la empresa. |  |  |  |  | No |  |
| 11.2.6 | Seguridad de equipos y activos fuera de las instalaciones | Aplicar la misma seguridad que se realiza a los equipos dentro de la empresa | Se cubrirá con el control C022. |  |  |  |  | No |  |
| 11.2.7 | Disposición segura o reutilización de equipos | Se debe proteger la información confidencial de equipos en desuso o cuando son dados de baja. | No aplica a la empresa. |  |  |  |  | No |  |
| 11.2.8 | Equipos de usuario desatendidos | Establecer políticas para equipos cuando los usuarios no están presentes, evitando así el acceso no autorizado o robo de información. |  | X | X | X |  | Si | Los sistemas de información han sido configurados con bloqueo de sesión automático. **Control C026.** |
| 11.2.9 | Política de escritorio limpio y pantalla limpia | Definir procedimientos para que los escritorios estén libres de papeles, medios de almacenamiento que puedan permitir filtración de información, además políticas de pantallas limpias. |  | X | X | X | X | Si | Los escritorios deben permanecer libre de documentos con información confidencial. **Control C027.** |
| 12 | Seguridad de las operaciones | | | | | | | | |
| 12,1 | Procedimientos operacionales y responsabilidades | | | | | | | | |
| 12.1.1 | Procedimientos de operación documentados | Los procedimientos deben estar documentados y puestos al alcance de todos, también manuales de operaciones específicas |  |  |  | X | X | Si | Las políticas y documentación propia de la empresa en lo que respecta a procesos de negocio se encuentran en una carpeta compartida al cual toda la organización tiene acceso. **Control C028.** |
| 12.1.2 | Gestión de cambios | Establecer políticas donde los cambios sean realizados por personal autorizado, además deben quedar soportados para llevar un control para evitar contratiempos. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 12.1.3 | Gestión de capacidad | Se debe realizar un monitoreo de los recursos de tal forma que no afecten la operación, algunos pueden ser capacidad de banda ancha, circuitos descalibrados que afecten el fluido eléctrico, equipos de cómputo lentos. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 12.1.4 | Separación de los ambientes de desarrollo, pruebas y operación | Los ambientes de desarrollo prueba y operación deben estar aislados, con restricciones de acceso con el fin de evitar cambios o modificaciones no autorizadas. | No aplica a la empresa. |  |  |  |  | No |  |
| 12,2 | Protección contra códigos maliciosos | | | | | | | | |
| 12.2.1 | Controles contra códigos maliciosos | Los equipos de cómputo deben contar con software contra código malicioso, el cual se debe actualizar constantemente con el fin actualizar parches que mitiguen las nuevas vulnerabilidades. |  |  |  | X |  | Si | Se revisará que los activos de software deben contar con un antivirus actualizado. **Control C029.** |
| 12,3 | Copias de respaldo | | | | | | | | |
| 12.3.1 | Respaldo de información | Se debe realizar respaldo de la información, además se deben realizar pruebas para comprobar que estos cumplen con las políticas de respaldo- |  |  |  | X | X | Si | Se debe generar a los activos de software una copia de respaldo de manera mensual, esta debe ser revisada y almacenada en un lugar ajeno al centro de operaciones. **Control C030.** |
| 12,4 | Registro y seguimiento | | | | | | | | |
| 12.4.1 | Registro de eventos | Se debe llevar un control de los eventos con el fin de establecer procedimientos que ayuden a repararlos o eliminarlos definitivamente, con el fin de que no se vuelvan a presentar | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 12.4.2 | Protección de la información de registro | Se debe proteger la información de registro de personal no autorizado, sólo el administrador o encargado será quien pueda tener acceso a estos, se deben realizar copias de logs. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 12.4.3 | Registros del administrador y del operador | Todas las tareas que desarrollen el administrador y el operador del sistema de información deben estar registradas, además se debe realizar un respaldo de estos registros. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 12.4.4 | sincronización de relojes | Los relojes de los dispositivos que intervienen en el procesamiento de información deben estar sincronizados. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 12,5 | Control de software operacional | | | | | | | | |
| 12.5.1 | Instalación de software en sistemas operativos | La instalación de software debe estar controlada, de tal forma que sólo las personas autorizadas puedan realizar estas tareas, además deben quedar registradas. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 12,6 | Gestión de la vulnerabilidad técnica | | | | | | | | |
| 12.6.1 | Gestión de las vulnerabilidades técnicas | Se deben establecer procedimientos que minimicen las vulnerabilidades a que están expuestos los activos tecnológicos. | La probabilidad de error en las aplicaciones de mediplus es mínima pues son sistemas de terceros que han demostrado estabilidad. |  |  |  | X | No |  |
| 12.6.2 | Restricciones sobre la instalación de software | La instalación de software debe estar controlada, de tal forma que sólo las personas autorizadas puedan realizar estas tareas, además deben quedar registradas. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 12,7 | Consideraciones sobre auditorias de sistemas de información | | | | | | | | |
| 12.7.1 | Información controles de auditoría de sistemas | Se deben establecer procedimientos que permitan el buen uso de las herramientas de auditoría a los sistemas, pero siempre procurando minimizar la interrupción del servicio a causa de estas. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 13 | Seguridad de las comunicaciones | | | | | | | | |
| 13,1 | Gestión de la seguridad de las redes | | | | | | | | |
| 13.1.1 | Controles de redes | Se deben instalar dispositivos o software que permita controlar el acceso a la red como Firewall, Ids, autenticación para su ingreso |  |  |  | X | X | Si | Se cuenta con un directorio activo el cual requiere autenticación para el acceso a los activos de software. **Control C031.** |
| 13.1.2 | Seguridad de los servicios de red | Establecer controles de acceso, acuerdos de servicio en su utilización, monitoreo constante para detectar intrusos | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 13.1.3 | Separación en las redes | Es necesario loa separación de las redes como la intranet de la red con acceso a internet, para lo cual se debe implementar un DMZ | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 13,2 | Transferencia de información | | | | | | | | |
| 13.2.1 | Políticas y procedimientos de transferencia de información | Se deben establecer todas las políticas que sean necesarias para proteger la información en el momento de ser transferida (intercambio de información), permitiendo integridad y confidencialidad. | No aplica a la empresa. |  |  |  |  | No |  |
| 13.2.2 | Acuerdos sobre transferencia de información | Se deben establecer controles que permitan respetar acuerdos de intercambio o transferencia de información | No aplica a la empresa. |  |  |  |  | No |  |
| 13.2.3 | Mensajería electrónica | Deben existir controles sobre el uso adecuado de la mensajería electrónica, para ello se deben instalar programas que detecten antivirus y spam, además se debe existir capacitación sobre situaciones donde existan correos sospechosos, también políticas del uso adecuado de los recursos, en este caso uso del correo electrónico sólo para el desarrollo de las funciones asignadas. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 13.2.4 | Acuerdos de confidencialidad o de no divulgación | Se deben cumplir las políticas de confidencialidad de la información, las cuáles fueron aceptadas en el momento de la firma del contrato. | Se cubrirá con el control 7.1.2 |  |  |  |  | No |  |
| 14 | Adquisición, desarrollo y mantenimientos de sistemas | | | | | | | | |
| 14,1 | Requisitos de seguridad de los sistemas de información | | | | | | | | |
| 14.1.1 | Análisis y especificación de requisitos de seguridad de la información | Las especificaciones de requisitos se deben tener en cuenta cuando se vaya a realizar un cambio o implementar un nuevo sistema de información | No aplica a la empresa. |  |  |  |  | No |  |
| 14.1.2 | Seguridad de servicios de las aplicaciones en redes publicas | Se debe implementar seguridad en los servicios que viajan por redes públicas tales como autenticación, manejo de cookies, sesiones, pki, con el fin de garantizar la confiabilidad de la información | No aplica a la empresa. |  |  |  |  | No |  |
| 14.1.3 | Protección de transacciones de los servicios de las aplicaciones | Se debe implementar seguridad en los servicios que viajan por redes públicas tales como autenticación, manejo de cookies, sesiones, pki, con el fin de garantizar la confiabilidad de la información | No aplica a la empresa. |  |  |  |  | No |  |
| 14,2 | Seguridad en los procesos de desarrollo y soporte | | | | | | | | |
| 14.2.1 | Política de desarrollo seguro | Es importante establecer políticas de código seguro en el desarrollo de software, es aquí donde se deben implementar procedimientos de seguridad como paso de variables por cabecera, sesiones, entre otros, los cuáles deben blindar el sistema de información para evitar vulnerabilidades | No aplica a la empresa. |  |  |  |  | No |  |
| 14.2.2 | Procedimientos de control de cambios en sistemas | Todos los cambios que se realicen a los programas se deben documentar y quedar registrados, para lo cual se deben establecer procedimientos | No aplica a la empresa. |  |  |  |  | No |  |
| 14.2.3 | Revisión técnica de las aplicaciones después de cambios en la plataforma de operación | Se deben realizar pruebas a las aplicaciones que han sido modificadas, con el fin de evitar alteraciones en la prestación del servicio o mal funcionamiento a causa del desarrollo. | No aplica a la empresa. |  |  |  |  | No |  |
| 14.2.4 | Restricciones en los cambios a los paquetes de software | Los cambios o modificaciones que se le realizan a las aplicaciones deben estar restringidos con el fin de evitar fallas no deseadas. | No aplica a la empresa. |  |  |  |  | No |  |
| 14.2.5 | Principios de construcción de sistemas seguros | Establecer procedimientos y políticas que permitan la construcción de aplicaciones seguras | No aplica a la empresa. |  |  |  |  | No |  |
| 14.2.6 | Ambiente de desarrollo seguro | Los ambientes de desarrollo deben estar aislados y contar con todas las medidas de seguridad en cuanto a control de acceso a la información y a las instalaciones | No aplica a la empresa. |  |  |  |  | No |  |
| 14.2.7 | Desarrollo contratado externamente | Cuando se adquieran sistemas externos, realizar seguimiento, es necesario validarlos antes de ponerlos en funcionamiento | No aplica a la empresa. |  |  |  |  | No |  |
| 14.2.8 | Pruebas de seguridad de sistemas | Someter los sistemas a pruebas con el fin de identificar vulnerabilidades, se podría contemplar pruebas de hacking ético. | No aplica a la empresa. |  |  |  |  | No |  |
| 14.2.9 | Prueba de aceptación de sistemas | Someter los sistemas a pruebas con el fin de identificar vulnerabilidades, se podría contemplar pruebas de hacking ético. | No aplica a la empresa. |  |  |  |  | No |  |
| 14,3 | Datos de prueba | | | | | | | | |
| 14.3.1 | Protección de datos de prueba | Hay que tener cuidado con los datos que se van a ingresar para realizarle pruebas a la aplicación, esto con el fin de evitar alguna fuga de información importante. | No aplica a la empresa. |  |  |  |  | No |  |
| 15 | Relación con los proveedores | | | | | | | | |
| 15,1 | Seguridad de la información en las relaciones con los proveedores | | | | | | | | |
| 15.1.1 | Política de seguridad de la información para las relaciones con proveedores | Igual que con los usuarios de la organización, con los proveedores se deben establecer acuerdos de confidencialidad, control de acceso a l información, seguridad física, intercambio de información entre otros para no ver afectada la seguridad de la información. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 15.1.2 | Tratamiento de la seguridad dentro de los acuerdos con proveedores | Definir acuerdos de confidencialidad | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 15.1.3 | Cadena de suministro de tecnología de información y comunicación | Se deben establecer acuerdos que permitan mitigar los riesgos de la seguridad de la información derivados de la cadena de suministro. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 15,2 | Gestión de la prestación de servicios con los proveedores | | | | | | | | |
| 15.2.1 | Seguimiento y revisión de los servicios de los proveedores | Las organizaciones deben monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 15.2.2 | Gestión de cambios en los servicios de proveedores | Se debe contar con otras alternativas de proveedores que permitan la continuidad del servicio en caso de cambio de proveedor | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 16 | Gestión de incidentes de seguridad de la información | | | | | | | | |
| 16,1 | Gestión de incidentes y mejoras en la seguridad de la información | | | | | | | | |
| 16.1.1 | Responsabilidad y procedimientos | Definir procedimientos que permitan una reacción rápida ante problemas generados por causa de la seguridad de la información. |  |  |  | X |  | Si | Se diseñó e implementó el documento de Política de Gestión de Incidentes en el cual se especifica el plan de respuesta ante los incidentes de seguridad de la información. **Control C032.** |
| 16.1.2 | Reporte de eventos de seguridad de la información | Se debe informar sobre eventos generados a causa de seguridad de la información con el fin de documentar la solución, es necesario llevar un registro de estos. |  |  |  | X |  | Si | Los incidentes de seguridad de la información serán registrados en el documento lógico "Incidentes de Seguridad de la Información" lo que permitirá trazabilidad. **Control C033.** |
| 16.1.3 | Reporte de debilidades de seguridad de la información | Informar oportunamente sobre eventos generados, con el fin de identificar recurrencias y debilidades en seguridad de la información. |  |  |  | X |  | Si | Se cubrirá con el control **C033.** |
| 16.1.4 | Evaluación de eventos de seguridad de la información y decisiones sobre ellos | Cada vez que se presente un evento se seguridad de la información es importante evaluar si será considerado como un incidente o no. | Todos los eventos serán considerados incidentes, por lo que no se hará distinción. |  |  |  |  | No |  |
| 16.1.5 | Respuesta a incidentes de seguridad de la información | Se debe establecer un proceso que permita establecer los pasos a seguir para atender el incidente. |  |  |  | X |  | Si | Se diseñó e implementó el documento de Política de Gestión de Incidentes, en la cual se indica el plan de respuesta ante los incidentes acorde a su alcance. **Control C034.** |
| 16.1.6 | Aprendizaje obtenido de los incidentes de seguridad de la información | La experiencia que se ha adquirido en resolver los incidentes, es pieza fundamental para reducir el impacto que pueda causar este incidente a la seguridad de la información | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 16.1.7 | Recolección de evidencia | Definir un procedimiento para documentar los incidentes de tal forma que exista una evidencia. |  |  |  | X |  | Si | Se ha definido un documento Excel, en una carpeta compartida, en la cual se registraran los incidentes que se suscitarán en la organización. **Control C035.** |
| 17 | Aspectos de seguridad de la información de la gestión de continuidad de negocio | | | | | | | | |
| 17,1 | Continuidad de seguridad de la información | | | | | | | | |
| 17.1.1 | Planificación de la continuidad de la seguridad de la información | Definir políticas que permita la gestión de la continuidad del negocio, aunque la organización presente una crisis |  |  |  | X |  | Si | Se cubrirá con el control **C032.** |
| 17.1.2 | Implementación de la continuidad de la seguridad de la información | Implementar procedimientos que permitan la continuidad del negocio ante situaciones imprevistas que podrían causar retrasos en la operación. |  |  |  | X |  | Si | Se diseñó e implementó el documento de Política de Gestión de Incidentes, la cual cuenta con procedimiento que permite la continuidad del negocio ante eventos que no permitan la operatividad del mismo. Se cuenta con documentación física que permite la continuidad del negocio. **Control C036.** |
| 17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | Realizar revisiones a los procedimientos implementados para la gestión de la continuidad del servicio para determinar si son efectivos o no. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 17,2 | Redundancias | | | | | | | | |
| 17.2.1 | Disponibilidad de instalaciones de procesamiento de información. | Es necesario establecer redundancias en las instalaciones donde se procesa la información con el fin de que no se vea afectada la disponibilidad de la información. |  |  |  | X |  | Si | El nivel de complejidad de la empresa no le permite tener un centro de datos redundante. En respuesta al riesgo se diseñó e implementó el documento de Política de Gestión de Copias de Respaldo Se cuenta con instalaciones alternas para la continuidad del negocio. **Control C037.** |
| 18 | Cumplimiento | | | | | | | | |
| 18,1 | Cumplimiento de requisitos legales y contractuales | | | | | | | | |
| 18.1.1 | Identificación de la legislación aplicable y de los requisitos contractuales | Definir el marco legal con el cual se debe regir la seguridad de la información. |  | X | X |  |  | Si | Se diseñó e implementó el documento de Política de Seguridad de la Información, en esta política se especifica las leyes que son consideradas: - Ley 26842 - 1997 - Ley General de Salud Concordad, Artículo 25.- Toda información relativa al acto médico que se realiza, tiene carácter reservado. - Ley 29733 - 2011 - Ley de Protección de Datos Personales, Artículo 16.- Seguridad del tratamiento de datos personales. Y Artículo 17.- Confidencialidad de Datos Personales. **Control C038.** |
| 18.1.2 | Derechos de propiedad intelectual | Cumplir a cabalidad las políticas de derechos de propiedad intelectual, software patentado. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 18.1.3 | Protección de registros | Procedimiento que permita la custodia de los registros ante situaciones de robo, modificación, divulgación. |  | X | X | X |  | Si | Se han determinado controles preventivos que aseguran la seguridad de los registros: Controles: C014, C015, C020, C021, C026 y C031. |
| 18.1.4 | Privacidad y protección de datos personales | Cumplir con las políticas de la protección de datos personales |  | X | X | X | X | Si | Se han determinado controles preventivos que aseguran la seguridad de los registros: Controles: C014, C015, C020, C021, C026 y C031. |
| 18.1.5 | Reglamentación de controles criptográficos | Cumplir con las normas relacionadas con controles criptográficos | No aplica a la empresa. |  |  |  |  | No |  |
| 18,2 | Revisiones de seguridad de la información | | | | | | | | |
| 18.2.1 | Revisión independiente de la seguridad de la información | Se debe revisar periódicamente el SGSI, estas revisiones deben ser adicionales a las establecidas en las políticas de seguridad de la información. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 18.2.2 | Cumplimiento con las políticas y normas de seguridad | La dirección debe revisar los cumplimientos de las políticas de seguridad de la información establecidas de acuerdo a su área de responsabilidad. | No representa un riesgo crítico para la empresa. |  |  |  |  | No |  |
| 18.2.3 | Revisión del cumplimiento técnico | Se deben revisar que todo el personal conoce y cumple con las políticas de seguridad de la información |  |  |  |  |  | Si | Se debe realizar revisiones anuales al sistema de gestión de seguridad de la información. **Control C039.** |