**GESTIÓN DE RIESGOS CIBERNÉTICOS**

**OSCAR CAMARGO**

**JOSE GALVIS**

**JAIME ZAMUDIO**

**CARLOS RODRIGUEZ**

**WILFREDO SAMBONI**

**MAESTRIA DE CIBERSEGURIDAD Y CIBERDEFENSA**

**GESTIÓN DE RIESGOS CIBERNETICOS**

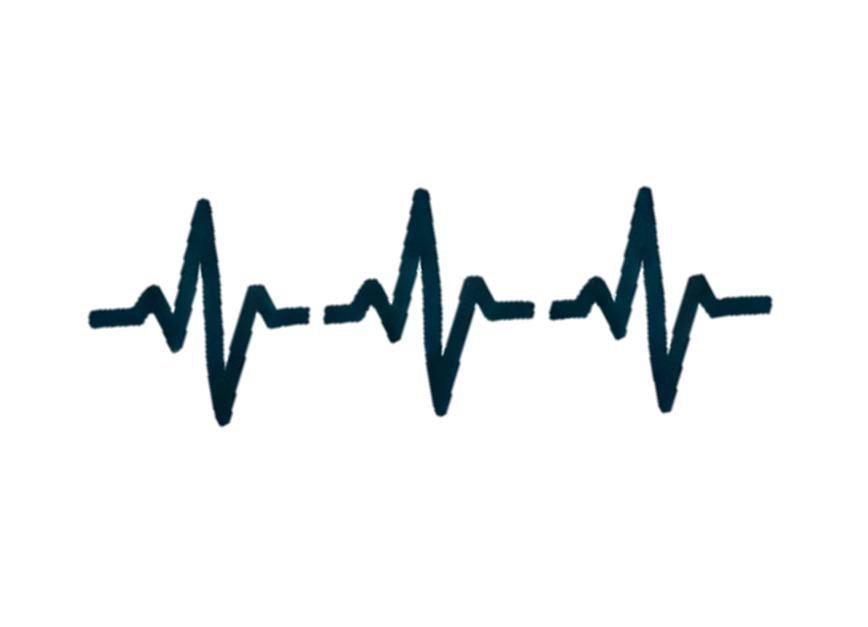
**ING. JAIDER OSPINA NAVAS**

**ESCUELA SUPERIOR DE GUERRA**

**“GENERAL RAFAEL REYES PRIETO”**

**BOGOTÁ D.C.**

1. **CONTEXTO DE LA ORGANIZACIÓN MEDIPLUS+ S.A.**



MEDIPLUS



* 1. **Definición del Alcance**

Mediplus+ S.A. busca implementar un **Sistema de Gestión de Seguridad de la Información (SGSI)** alineado con **ISO 27001:2022** para proteger la confidencialidad, integridad y disponibilidad de los datos médicos y administrativos de sus pacientes y colaboradores.

**Alcance del SGSI:**

* **Ámbito:** Todas las operaciones digitales, plataformas, sistemas de información y bases de datos que almacenan o procesan información médica y administrativa.
* **Ubicación:** Oficinas centrales, centros de atención médica y plataformas digitales en toda Colombia.
* **Activos Protegidos:** Historias clínicas, datos de pacientes, información financiera, sistemas de telemedicina y aplicaciones móviles.

**1.2 Análisis del Contexto de Mediplus+ S.A.**

**Factores Internos**

* **Modelo de negocio:** Medicina domiciliaria con servicios digitales avanzados.
* **Sistemas tecnológicos:** Plataformas en la nube para gestión de historias clínicas y telemedicina.
* **Datos Sensibles:** Manejo de datos personales, médicos y financieros conforme a la Ley 1581 de 2012.
* **Cultura organizacional:** Enfoque en la seguridad del paciente y cumplimiento normativo.

**Factores Externos**

* **Regulación Colombiana:** Cumplimiento de la Ley 1581 de Protección de Datos y normas de la **Superintendencia de Salud**.
* **Riesgos Cibernéticos:** Crecimiento del **ransomware en IPS**, con más de **20 ataques reportados en el último año** en Colombia.
* **Tendencias Globales:** Incremento del **40% en ataques a la salud** desde 2020 (Fuente: IBM X-Force Threat Intelligence).
  1. **Identificación de las Partes Interesadas**

| **Parte Interesada** | **Intereses / Expectativas** | **Requisitos de Seguridad** |
| --- | --- | --- |
| **Pacientes y Familiares** | Confidencialidad de datos médicos, continuidad en la atención. | Protección de datos personales (Ley 1581), acceso seguro a información. |
| **Médicos y Personal de Salud** | Acceso ágil y seguro a historias clínicas, confiabilidad en telemedicina. | Control de accesos, disponibilidad 24/7 de sistemas. |
| **Superintendencia de Salud** | Cumplimiento normativo, auditoría de protección de datos. | Adopción de estándares ISO 27001 y Ley 1581. |
| **Aseguradoras y EPS** | Seguridad en transmisión de datos financieros y clínicos. | Cifrado y autenticación en transferencias de datos. |
| **Proveedores Tecnológicos** | Integración con plataformas seguras, cumplimiento de SLA. | Cumplimiento con ISO 27001 y normas de ciberseguridad. |

**ANEXO: MATRIZ DOFA – DOCUMENTO EN EXCEL**

**Imagen que contiene señal, firmar, calle, reloj

Descripción generada automáticamente**

1. **LIDERAZGO Y COMPROMISO MEDIPLUS+**

**2.1 Compromiso de la alta dirección**

La alta dirección tiene un papel crucial en la toma de decisiones estratégicas, la gestión de recursos y la creación de la una cultura organizacional que garantice la excelencia en la atención medica de emergencia de la siguiente manera:

a) Garantizar la calidad en Atención Médica

La alta dirección tiene la responsabilidad e asegurarse que los servicios médicos que ofrece la empresa estén alineados con los estándares más altos de calidad lo que incluye dentro de sus servicios lo siguiente;

* Implementar y mantener protocolos médicos rigurosos
* Asegurar que el personal medico este en constante capacitación y actualización
* Fomentar la mejora continua y los procesos operativos para reducir los tiempos de respuesta y mejorar la atención al paciente

b) Cumplimiento normativo y regulatorio

c) Desarrollo y gestión de recursos

d) Seguridad y protección de los empleados y pacientes

d) Fomento de la innovación tecnológica

**2.2 Política de seguridad de la información**

La política de esta empresa debe ser robusta, integral y alineada con las mejores prácticas de industria, así como las normativas legales aplicables. Esto debido a que la información aplicada en el ámbito de emergencias medicas es de naturaleza critica, es esencial implementar medidas de seguridad que protejan la privacidad y la integridad de los datos por lo tanto se deben tener algunos aspectos importantes tales como;

* 1. Objetivo de la política
  2. Alcance
  3. Confidencialidad
  4. Integridad
  5. Disponibilidad
  6. Control de accesos
  7. Protección contra amenazas
  8. Capacitación y concienciación
  9. Cumplimiento de normativas
  10. Gestión de incidentes
  11. Revisión y mejora continua

**2.3 Asignación de roles y responsabilidades**

Para esta empresa, la asignación de roles y responsabilidades es esencial para asegurar una eficiente operación, la atención de calidad, y el cumplimiento de las normativas. Por lo tanto, los roles están claramente definidos y alienados con los objetivos estratégicos además con esto se asegura que las operaciones diarias y situaciones de emergencia se gestionen de forma eficaz.

Para dicha actividad se realizó un documento referido como asignación de roles en Excel.

1. **EVALUACIÓN DEL RIESGO**

**3.1 Identificación de Activos**

Para dicha actividad se realizó un Inventario de los Activos referidos en el documento Inventario de Activos de Excel.

**3.2 Análisis de Riesgos**

Para dicha actividad se realizó un Análisis y Gestión de riesgos referidos en el documento Análisis y Gestión de Riesgos de Excel.

**3.3 Tratamiento de los Riesgos**

Para dicha actividad se realizó un documento referido como Evaluación de Riesgos en Excel.

1. **IMPLEMENTACIÓN DE LOS CONTROLES**

**4.1 Adopción Controles**

**4.1.1. SEGURIDAD DE PERSONAS**

* **Seguridad en los Puestos de Trabajo.**

El área administrativa en cabeza de la persona delegada por el gerente administrativo en compañía del gerente TI adicionara las funciones y responsabilidades en materia de seguridad informática a la descripción de las responsabilidades de los puestos de trabajo. Estas incluirán las responsabilidades generales en la implementación y mantenimiento de las políticas de seguridad y las responsabilidades especificas con respecto a la protección de activos o procesos relacionados con la seguridad de la información.

* + - 1. **Compromiso de Confidencialidad.**

Como parte de los términos y condiciones iniciales de empleo, los empleados, cualquiera que sea su tipo de vinculación, deberán firmar un acuerdo de confidencialidad o de no divulgación en cuanto a lo que tiene que ver con el tratamiento de la información de MEDIPLUS. El área administrativa deberá guardar la copia firmada por el empleado en forma segura, asi mismo mediante el acuerdo de confidencialidad el empleado declara conocer y aceptar la existencia de algunas actividades que van a ser controladas y monitoreadas. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

* + - 1. **Términos y Condiciones de Empleo**

Los términos y condiciones del empleo deberán establecer las responsabilidades con respecto a la seguridad de la información. Cuando sea pertinente, los términos y condiciones deberán establecer que estas responsabilidades van más allá del horario laboral ya sea que el personal se encuentre en la oficina o realizando viajes de trabajo. Además, se incluirá la normativa legal por la violación de protección de datos o uso ilegal de software.

* + - 1. **Capacitación del Usuario**
         1. **Formación y Capacitación de la Seguridad de la Información.**

Todo el personal sin excepción alguna, y cuando sea necesario personal externo que tengan que ver o desempeñen funciones en MEDIPLUS en cuanto al manejo de la información, deberán recibir una adecuado y periódica capacitación en materia de normas, procesos y procedimientos de la seguridad informática. Estas capacitaciones deberán abarcar los requerimientos de seguridad y las normativas legales, asi como el uso correcto de los recursos en general, como son los puestos de trabajo. El área administrativa será la encargada de coordinar y programar las capacitaciones necesarias para cumplir la presente política. Cada trimestre se deberán revisar estas capacitaciones de acuerdo con el estado del arte del momento. La gerencia TI será la encargada de realizar el material necesario para realizar las capacitaciones. El personal que ingrese a MEDIPLUS deberá recibir este material, donde se explicara el comportamiento esperado en cuanto a lo que tiene que ver con la seguridad informática, antes de ser otorgados los privilegios al acceso a los sistemas de información correspondiente a sus funciones. Por otra parte, el Gerente TI deberá auditar los recursos técnicos por los cuales se informará al personal cualquier modificación o novedades en cuanto a la seguridad informática.

* + - 1. **Respuesta a Incidentes de la Seguridad de la Información**
         1. **Comunicación de Incidentes de la Seguridad de la Información.**

Cualquier incidente por más mínimo que sea relacionado a la seguridad de la información, deberá ser informado inmediatamente a la gerencia TI, mediante los canales estipulados. La gerencia TI deberá establecer un proceso y procedimiento formal de comunicación y respuesta a incidentes. Este proceso deberá incluir el tiempo en que debe ser informado a la gerencia TI el incidente ocurrido a su vez deberá indicar los recursos necesarios para investigar y solucionar el incidente también el seguimiento que se realizará.

* + - * 1. **Comunicación de debilidades de la Seguridad de la Información.**

Los empleados de MEDIPLUS al momento de conocer directa o indirectamente una debilidad en la seguridad de la información de la compañía, deberán registrar e informar inmediatamente al propietario de la información y a la gerencia TI la debilidad. A su vez queda prohibido realizar cualquier acción para demostrar o utilizar la debilidad sin la previa autorización del propietario de la información y la gerencia TI.

* + - * 1. **Comunicación y corrección a problemas en el Software.**

La gerencia TI será la encargada de establecer los procedimientos para la comunicación y corrección de los problemas de software, los cuales deberán tener lo siguiente:

1. Registrar los eventos y mensajes en pantalla.
2. Establecer las medidas necesarias ante una eventual anomalía.
3. Alertar inmediatamente a la gerencia TI y al responsable del activo.

Se prohíbe al personal desinstalar el software que supuestamente tiene la anomalía, a menos q estén autorizados formalmente por gerencia TI.

* + - * 1. **Retroalimentación de los Incidentes.**

El comité de seguridad de la información deberá definir un procedimiento el cual permita medir, documentar y monitorear los tipos y costos de los incidentes y/o anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes, para que sean evaluados a modo de establecer la necesidad de mejorar o agregar controles para evitar q sigan ocurriendo los incidentes y/o anomalías.

* + - * 1. **Procesos Disciplinarios**

Se seguirá el proceso disciplinario formal que indique el reglamento interno de la compañía o el contrato laboral para los empleados que violen las políticas, normas, procesos o procedimientos de la seguridad de la información.

**4.1.2. PERÍMETRO DE SEGURIDAD FÍSICA**

La protección física se lleva a cabo alrededor de las instalaciones donde se procesa la información así:

1. Existe una barrera física con talanquera la cual solo se habilita mediante una tarjeta de ingreso para el acceso al edificio.
2. Puertas físicas y biométrico para el ingreso a las oficinas.
3. Paredes sólidas y de vidrio para el ingreso a los diferentes departamentos.
4. Puertas de vidrio para el acceso a las gerencias.
5. Puerta de vidrio para el acceso de cuartos de equipos que solo puede ser abierta por el gerente TI y/o el coordinador TI.

Se implementaron los siguientes lineamientos.

1. Las paredes externas son sólidas y la puerta que comunican con el exterior esta debidamente protegida contra accesos no autorizados mediante el uso de un biométrico.
2. Se verifica la existencia de un área de recepción atendida por personal.
3. Se definen las áreas de procesamiento de información, las cuales son físicamente solidas.
4. Existe un comité de brigadas el cual tiene claramente los procedimientos de evacuación.
5. Se ha capacitado constantemente al personal e, que se debe hacer en caso de emergencias.

**4.1.2.1. Controles de acceso físico**

Las áreas de procesamiento de información se resguardan mediante el empleo de controles físicos los cuales fueron determinados por la gerencia TI y tiene las siguientes características:

1. Se cuenta con un circuito cerrado de televisión con cámaras en todas las áreas.
2. Se controla el acceso a la información clasificada y a las instalaciones de procesamientos de información exclusivamente al personal autorizado.

**4.1.2.2.** Protección de Oficinas.

Se cuentan con las medidas de seguridad requeridas por las normativas de ley en materia de sanidad y seguridad como son por ejemplo el sistema contraincendios además del cumplimiento de certificaciones como son el RETIE y el RETILAP.

Se establecieron las siguientes medidas de protección para las áreas protegidas:

1. Las instalaciones críticas se encuentran en lugares a los cuales no pueda acceder personal no autorizado.
2. Los sitios donde se realizan actividades de procesamiento de información son discretos.
3. Equipos como son las impresoras y fotocopiadoras se encuentran ubicadas dentro del área protegida pero no es necesario el acceso, para evitar pérdidas de información.

**4.1.2.3. Ubicación y Protección de Activos fijos**

Los activos físicos que almacenan o procesan información se encuentran debidamente ubicados en los puestos de trabajo o el área a que corresponda cumpliendo la normativa de ley con respecto a distancias necesarias, además se tuvo en cuenta lo siguiente:

1. Los activos se encuentran ubicados en sitios donde se minimiza el acceso innecesario.
2. Los activos de procesamiento y almacenamiento de información se encuentran ubicados en sitios donde se permite la supervisión del uso.

**4.1.2.4. Suministros de Energía**

MEDIPLUS cumple con la normativa RETIE (Reglamento Técnico de Instalaciones Eléctricas) y su principal objetivo que es garantizar la seguridad de las personas previniendo, minimizando y eliminando los riesgos de origen eléctrico. Asimismo, los interruptores de emergencia se encuentran ubicados cerca de las salidas de emergencia con el fin de facilitar un corte rápido de energía. También cuenta con una iluminación de emergencia en caso de fallas en el suministro de energía. Se cuentan con protección contra descargas eléctricas en toda la oficina.

Para asegurar la continuidad el servicio deberá realizar lo siguiente:

* Implementar un suministro de energía ininterrumpible (UPS) para asegurar el apagado regulado, sistemático y la ejecución continua de los equipos que almacenen y/o procesen información. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida

**4.1.2.5. Mantenimiento de Equipos**

El mantenimiento de los equipos solo es realizado por el personal capacitado de TI, mediante previa información al propietario del activo. MEDIPLUS deberá realizar un registro de las fallas encontradas y todo el mantenimiento preventivo o correctivo que se haya realizado.

**4.1.2.6. Políticas de Escritorios y Pantallas Limpias.**

MEDIPLUS deberá adoptar una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento extraíbles además de una política de pantallas limpias en las instalaciones de procesamiento de información. Se aplicarán las siguientes directrices:

* Almacenar bajo llave, cuando corresponda, los documentos en papel y medios informáticos cuando no sean utilizados, especialmente en horarios no laborales.
* Almacenar bajo llave la información sensible de MEDIPLUS, puede ser en una caja fuerte cuando no sean utilizados, especialmente en horarios no laborales.
* Desconectar de la red los sistemas de información que tienen funciones criticas cuando no sean utilizados, especialmente en horarios no laborales.
* Retirar inmediatamente la información sensible o confidencial una vez q ha sido impresa.

**4.1.2.7. Retiro de los Bienes**

Los equipos, la información y el software no pueden ser retirados de MEDIPLUS sin autorización formal de las gerencias.

**4.1.3. CONTROL DE ACCESOS**

ANEXO: MATRIZ CONTROL ACCESOS – EXCEL

A. El acceso al cuarto de redes, servidores y áreas de trabajo que contengan información sensible o crítica, está restringido y solamente el personal autorizado podrá acceder a estos lugares.

B. Documentos impresos que contengan información sensible o crítica deben estar siempre almacenados o guardados en lugares que garanticen su seguridad, conservación y protejan su acceso inclusive durante horas no laborales.

C. Siempre que no se esté utilizando el computador debe cerrarse la sesión de trabajo para evitar que un empleado no autorizado acceda al sistema.

D. Es responsabilidad del colaborador evitar en todo momento la fuga de la información de MEDIPLUS que se encuentre almacenada en los equipos que tenga asignados.

E. Cualquier persona que tenga acceso a las instalaciones de MEDIPLUS deberá registrar al momento de su entrada el equipo de cómputo y herramientas que no sean propiedad de esta, el cual podrán retirar el mismo día, para esto deberá diligenciarse el documento denominado “Planilla de Ingreso y Salida de Activos Tecnológicos” dispuesta en la recepción.

F. Los colaboradores no deben mover o reubicar los equipos de cómputo, instalar o desinstalar dispositivos, ni retirar sellos de estos sin la autorización respectiva.

G. La Gerencia Administrativa y Financiera será la encargada de generar el resguardo y asegurar la firma del empleado como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el Departamento de TI. El movimiento o retiro de equipos por traslado, reemplazo o baja debe ser informado a la Gerencia Administrativa y Financiera, por el Departamento de TI y el empleado responsable del activo.

H. El equipo de cómputo asignado deberá ser para uso exclusivo de las funciones de MEDIPLUS.

I. Será responsabilidad del colaborador solicitar al Departamento de TI la asesoría necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

J. Mientras se opera el equipo de cómputo solamente se permite ingerir líquidos en los vasos o recipientes facilitados por la compañía.

K. Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o de la CPU.

L. Se debe mantener el computador en un entorno limpio y sin humedad.

N. El colaborador debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos.

M. Queda prohibido que el usuario abra o desarme los equipos de cómputo. Únicamente el personal autorizado por el Departamento de TI podrá llevar a cabo los servicios y reparaciones al equipo de cómputo.

O. Los colaboradores y el Departamento de TI deberán asegurarse de respaldar la información que consideren relevante y borrarla cuando el equipo de cómputo sea enviado a reparación, evitando así la pérdida involuntaria de información, derivada del proceso de reparación.

P. El colaborador que tenga bajo su custodia algún equipo de cómputo será responsable de su uso y conservación; en consecuencia, responderá con su propio patrimonio por la pérdida, daño o deterioro que ocurra a los equipos cuando el hecho acontezca por negligencia o culpa del trabajador.

Q. El resguardo para los portátiles tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

R. El empleado deberá dar aviso inmediato de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo a la Gerencia Administrativa y Financiera.

S. Si algún área por requerimiento muy específico tiene la necesidad de contar con un dispositivo especial o específico, su instalación deberá ser autorizada por la Gerencia General, con el apoyo técnico del Departamento de

TI.

T. Deberá configurarse el computador de tal manera que durante un tiempo de inactividad éste sea bloqueado automáticamente y se requiera para el reinicio de actividades el ingreso de una clave o password, el tiempo de inactividad se ha establecido en 5 minutos.

**4.1.4. CONTROL DE CIFRADOS**

Para garantizar la seguridad de las comunicaciones y la protección de la información manejada por la central telefónica de MEDIPLUS, se han implementado diversos controles de cifrado que aseguran tanto las transmisiones de voz como los datos almacenados y en tránsito. A continuación, se detallan las acciones adoptadas:

**4.1.4.1** Cifrado de Llamadas: Todas las comunicaciones de voz que pasan a través de nuestra infraestructura VoIP están cifradas utilizando los siguientes protocolos:

**4.1.4.2** TLS: Se ha habilitado TLS para cifrar todas las señales SIP (Session Initiation Protocol) entre los teléfonos IP, los dispositivos de los empleados y el servidor PBX, asegurando la confidencialidad de las señales de control.

**4.1.4.3** SRTP: El tráfico de audio en tiempo real es cifrado utilizando SRTP (Secure Real-Time Transport Protocol), lo que garantiza que las conversaciones telefónicas estén protegidas frente a cualquier intento de interceptación durante su transmisión.

**4.1.4.4** Cifrado de Datos en Reposo: Todos los registros de llamadas, grabaciones y detalles de clientes almacenados en nuestros servidores están protegidos mediante cifrado de alta seguridad. Las acciones implementadas incluyen:

**4.1.4.5** AES con claves de 256 bits: Se ha adoptado el estándar AES con claves de 256 bits para cifrar los datos almacenados, asegurando que solo personal autorizado pueda acceder a la información sensible.

**4.1.4.6** Control de acceso robusto: Se han establecido políticas estrictas de control de acceso a los datos cifrados, con permisos limitados a empleados específicos que requieren acceso para realizar tareas relacionadas con el servicio.

**4.1.4.7** Cifrado de Datos en Tránsito: Para proteger la integridad de los datos en tránsito a través de redes públicas y privadas, se han implementado las siguientes medidas:

**4.1.4.8**VPN: Todos los empleados remotos y dispositivos móviles que necesitan conectarse a la infraestructura de la central telefónica utilizan una VPN (Red Privada Virtual) cifrada, lo que garantiza que todas las transmisiones de datos se realicen de manera segura.

**4.1.4.9**HTTPS para Interfaces Web: Las interfaces web de administración y gestión de la central telefónica están protegidas con HTTPS, utilizando certificados SSL/TLS válidos para evitar la intercepción de credenciales y datos administrativos.

**4.1.4.10** Gestión de Claves y Control de Acceso: Se ha implementado una infraestructura de gestión de identidades y claves para garantizar que solo personal autorizado tenga acceso a la información cifrada y a las configuraciones de la central telefónica:

**4.1.4.11**Autenticación Multifactor (MFA): Todos los accesos a las interfaces de administración de la central telefónica requieren autenticación multifactor, lo que añade una capa adicional de seguridad contra accesos no autorizados.

**4.1.4.12** Gestión segura de claves criptográficas: Las claves criptográficas son gestionadas mediante un módulo de seguridad de hardware (HSM), que protege el ciclo de vida de las claves y garantiza su uso adecuado y seguro.

**4.1.4.13** Cumplimiento de Normativas y Auditoría: La implementación de los controles de cifrado también se alinea con las normativas locales e internacionales de protección de datos y privacidad de las comunicaciones:

**4.1.4.14** Auditoría continua: Se ha implementado un sistema de auditoría que registra todas las actividades relacionadas con el acceso y manejo de datos cifrados, permitiendo detectar cualquier acceso no autorizado o intento de vulneración.

**4.1.4.15** Cumplimiento de la legislación: Todos los procesos de cifrado y manejo de información están en cumplimiento con la normativa aplicable, incluyendo las leyes locales de protección de datos y las mejores prácticas internacionales de seguridad.

**4.1.4.16** Revisión Periódica de Seguridad: Para asegurar que los controles de cifrado se mantengan efectivos, se realizan auditorías y revisiones periódicas de la infraestructura:

**4.1.4.17** Pruebas de penetración: Se llevan a cabo pruebas de penetración regulares para identificar vulnerabilidades y corregirlas antes de que puedan ser explotadas.

**4.1.4.18** Actualizaciones constantes: Todos los sistemas involucrados en la transmisión y almacenamiento de datos cifrados se actualizan regularmente para protegernos de nuevas amenazas de seguridad.

**4.1.4.19** Protección de Dispositivos: Finales Además de las medidas mencionadas, todos los dispositivos empleados por los usuarios para acceder a la central telefónica están protegidos:

**4.1.4.20** Cifrado de dispositivos: Todos los dispositivos móviles y estaciones de trabajo utilizados por los empleados de MEDIPLUS están cifrados para proteger los datos almacenados en ellos, incluso en caso de pérdida o robo.

1. **CAPACITACIÓN Y CONCIENTIZACIÓN**

La capacitación y concientización del personal es uno de los pilares fundamentales para garantizar la seguridad de la información y el cumplimiento de las normativas en cualquier organización. En este documento, se detallarán las estrategias y prácticas implementadas para la formación del personal en el manejo seguro de la información, tomando como referencia los estándares y procedimientos aplicados en la gestión segura de claves criptográficas y el cumplimiento de normativas, dentro del marco de un Sistema de Gestión de Seguridad de la Información (SGSI).

El principal objetivo de la capacitación es dotar a los empleados de los conocimientos y habilidades necesarios para proteger la información sensible y cumplir con las normativas legales. Esto incluye:

* Comprensión de la Seguridad de la Información: Proveer una base sólida sobre los conceptos de seguridad de la información, incluyendo las amenazas, vulnerabilidades y medidas de protección.
* Manejo Seguro de Datos: Asegurar que los empleados conozcan las técnicas y prácticas para el manejo seguro de datos, incluyendo el cifrado y la protección de dispositivos.
* Conformidad Normativa: Garantizar que el personal esté al tanto de las leyes y regulaciones aplicables, así como de las políticas internas de la empresa.
  1. **Estrategias de Capacitación**

Para lograr estos objetivos, se implementan diversas estrategias de capacitación, entre las que se incluyen:

## **Sesiones de Formación Presenciales**

La organización ofrece sesiones de formación presenciales que son impartidas por expertos en seguridad de la información. Estas sesiones cubren temas clave como:

* Conceptos Básicos de Seguridad: Introducción a los principios de la seguridad de la información y la importancia de la protección de datos.
* Uso Seguro de Tecnología: Instrucciones sobre el uso seguro de herramientas y dispositivos tecnológicos, incluyendo la gestión de contraseñas y el cifrado de datos.
* Prácticas de Seguridad en el Trabajo Diario: Orientación sobre cómo aplicar las mejores prácticas de seguridad en las actividades cotidianas.

## **5.1.2 Capacitación en Línea**

Para complementar las sesiones presenciales, se ofrece capacitación en línea a través de plataformas de e-learning. Estas plataformas permiten a los empleados acceder a módulos interactivos, videos y cuestionarios en su propio tiempo y ritmo. Los temas incluyen:

* Actualización de Conocimientos: Módulos que se actualizan regularmente para reflejar las últimas amenazas y técnicas de protección.
* Evaluaciones Continuas: Cuestionarios y exámenes periódicos para evaluar el conocimiento y comprensión de los empleados.
* Recursos Adicionales: Acceso a materiales de referencia y guías prácticas para profundizar en los temas tratados.

## **5.1.3 Simulacros y Ejercicios de Seguridad**

Se realizan simulacros y ejercicios de seguridad para evaluar la respuesta del personal ante situaciones de riesgo. Estos ejercicios ayudan a:

* Identificar Debilidades: Detectar áreas de mejora en la formación y preparación del personal.
* Refinar Procedimientos: Ajustar y mejorar los procedimientos de seguridad basados en los resultados de los simulacros.
* Reforzar el Aprendizaje: Proporcionar una experiencia práctica que refuerce los conocimientos adquiridos durante la capacitación.

## **5.1.4 Campañas de Concientización**

Las campañas de concientización juegan un papel crucial en mantener al personal informado y vigilante. Estas campañas incluyen:

* Boletines Informativos: Envío regular de boletines con noticias, consejos y actualizaciones sobre seguridad de la información.
* Material Visual: Carteles, infografías y otros materiales visuales que se colocan en áreas comunes para recordar las mejores prácticas de seguridad.
* Eventos y Talleres: Organización de eventos especiales y talleres interactivos para fomentar una cultura de seguridad.

# **5.1.5 Evaluación y Mejora Continua**

La efectividad de la capacitación y concientización es evaluada regularmente a través de:

* Auditorías de Conocimiento: Revisiones periódicas del conocimiento y habilidades del personal.
* Feedback de los Empleados: Recopilación de comentarios y sugerencias de los empleados para mejorar los programas de formación.
* Revisión de Incidentes: Análisis de incidentes de seguridad para identificar fallos y mejorar las prácticas de capacitación.

La capacitación y concientización del personal es esencial para proteger la información y cumplir con las normativas de seguridad. Mediante la implementación de programas de formación integrales y estrategias de concientización efectivas, se puede asegurar que todos los empleados estén preparados para enfrentar los desafíos de seguridad y contribuir a un entorno de trabajo seguro y conforme a la legislación vigente.

1. **MONITOREO Y EVALUACIÓN**

**7.1 Seguimiento a los Desempeños**

El seguimiento a los desempeños es fundamental para evaluar de manera continua la efectividad de las estrategias de capacitación y concientización en seguridad implementadas por la empresa MedPlus. Mediante el seguimiento sistemático, se puede asegurar que todos los empleados comprendan y apliquen las mejores prácticas de seguridad en su trabajo diario. Aquí se presenta un marco detallado para llevar a cabo el seguimiento a los desempeños:

**7.1.1 Indicadores Clave de Desempeño (KPIs)**

El establecimiento de Indicadores Clave de Desempeño (KPIs) permite medir el progreso y la efectividad de las iniciativas de seguridad. Algunos KPIs esenciales incluyen:

* Porcentaje de empleados que completan los programas de capacitación de seguridad.
* Nivel de conocimiento demostrado en auditorías de conocimiento.
* Número de incidentes de seguridad reportados y su gravedad.
* Tiempo de respuesta ante incidentes de seguridad.
* Número de sugerencias y feedback recibido de los empleados.

**7.1.2 Revisiones Periódicas de Desempeño**

Las revisiones periódicas de desempeño implican la evaluación regular del conocimiento y habilidades del personal mediante:

* Auditorías de Conocimiento: Realización de pruebas y evaluaciones para comprobar el entendimiento de las políticas y procedimientos de seguridad.
* Observaciones en el Lugar de Trabajo: Supervisión directa de las prácticas de los empleados para asegurar el cumplimiento de las normas de seguridad.
* Reuniones de Desempeño: Reuniones individuales y grupales para discutir el rendimiento en seguridad y proporcionar retroalimentación constructiva.

**7.1.3 Feedback Continuo de los Empleados**

El feedback continuo de los empleados es esencial para identificar áreas de mejora y adaptar los programas de capacitación. Se pueden implementar las siguientes estrategias:

* Encuestas y Cuestionarios: Distribución regular de encuestas para recopilar opiniones sobre la efectividad de las formaciones.
* Sesiones de Feedback: Organización de sesiones de retroalimentación donde los empleados puedan expresar sus inquietudes y sugerencias.
* Canales de Comunicación Abiertos: Mantener líneas de comunicación abiertas como correos electrónicos y buzones de sugerencias.

**7.2 Auditorías Internas**

Las auditorías internas son una herramienta crucial para evaluar el cumplimiento de las políticas de seguridad y la efectividad de las estrategias de capacitación y concientización. A través de auditorías rigurosas, MedPlus puede identificar deficiencias y áreas de mejora, asegurando que las prácticas de seguridad se mantengan actualizadas y efectivas. A continuación, se describe un enfoque detallado para la realización de auditorías internas:

**7.2.1 Planificación de Auditorías**

La planificación eficaz de auditorías incluye:

* Programación Regular: Establecer un calendario de auditorías periódicas para revisar las prácticas de seguridad en intervalos regulares.
* Definición de Objetivos: Clarificar los objetivos y alcances de cada auditoría, enfocándose en áreas críticas como la gestión de datos, control de acceso y respuesta a incidentes.
* Selección de Auditores: Designar auditores internos capacitados y, cuando sea necesario, contratar auditores externos para una evaluación imparcial.

**7.2.3 Ejecución de Auditorías**

Durante la ejecución de auditorías, se deben seguir estos pasos:

* Recolección de Datos: Recopilar información detallada sobre las prácticas de seguridad mediante entrevistas, revisiones documentales y observaciones directas.
* Análisis de Cumplimiento: Evaluar el nivel de cumplimiento de las políticas y procedimientos de seguridad establecidos por la empresa.
* Identificación de No Conformidades: Detectar cualquier incumplimiento o desviación de las prácticas de seguridad y documentarlas adecuadamente.

**7.2.4 Informes de Auditoría**

La elaboración de informes de auditoría claros y detallados es crucial para comunicar los hallazgos y recomendaciones:

* Resumen Ejecutivo: Incluir un resumen de los hallazgos principales y las recomendaciones críticas para la alta dirección.
* Detalles de Hallazgos: Proporcionar una descripción detallada de las áreas de no conformidad y las evidencias encontradas.
* Recomendaciones de Mejora: Sugerir acciones correctivas y preventivas para abordar las deficiencias identificadas.

## Acciones Correctivas y Preventivas

Implementar acciones correctivas y preventivas es esencial para mejorar continuamente las prácticas de seguridad:

* Plan de Acción: Desarrollar y ejecutar un plan de acción para abordar las no conformidades identificadas durante la auditoría.
* Seguimiento y Verificación: Realizar un seguimiento regular para asegurar que las acciones correctivas se han implementado efectivamente.
* Revisión y Actualización: Revisar y actualizar las políticas y procedimientos de seguridad basándose en los resultados de las auditorías.

1. **MEJORA CONTINUA**

**8.1 Gestión de Incidentes**

El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

Las organizaciones cuentan con innumerables activos de información, cada uno expuesto a sufrir incidentes de seguridad. Resulta necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares.

Se establecen las responsabilidades y procedimientos para manejar los eventos y debilidades en la seguridad de información de una manera efectiva y una vez que hayan sido comunicados. Se debería aplicar un proceso de mejora continua en respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes en la seguridad de información.

Cuando se requieran evidencias, éstas deben ser recogidas para asegurar el cumplimiento de los requisitos legales

Diagrama, Icono

Descripción generada automáticamente

**8.1.1 Gestión de incidentes de seguridad de la información y mejoras**

El objetivo es asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información incluyendo la comunicación de los eventos de seguridad y debilidades.

**8.1.2 Riesgos asociados**

Las revisiones post-incidentes y los casos de estudio para incidentes serios, tales como fraudes, ilustran los puntos débiles de control, identifican oportunidades de mejora y conforman por sí mismos un mecanismo eficaz de concienciación en seguridad.

Se debe establecer un informe formal de los eventos y de los procedimientos de escalado.

Todos los empleados, contratistas y terceros deberían estar al tanto de los procedimientos para informar de los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos de información.

Se les debería exigir que informen de cualquier evento o debilidad en la seguridad de información lo más rápido posible y al punto de contacto designado.

Establezca y dé a conocer un punto de comunicación como el helpdesk habitual de TI para que la gente pueda informar de incidentes, eventos y problemas de seguridad.

Una falta de control en estos aspectos permite la materialización de potenciales amenazas, entre otras posibles, como:

- Daños físicos (agua, fuego, polución, accidentes, destrucción de equipos, polvo, corrosión, congelación, etc.)

- Pérdida de servicios esenciales (energía eléctrica, telecomunicaciones, aire acondicionado, agua, etc.)

- Afectaciones por radiación (electromagnéticas, térmicas, etc)

- Compromiso de información (intercepción, espionaje en remoto, espionaje en proximidad, robo de equipos o documentos, recuperación desde medios reciclados o deshechados, divulgación, datos de fuentes no fiables, manipulación de hardware, manipulación de software, etc.)

- Fallos técnicos (falla o mal funcionamiento del equipo, saturación del sistema de información, mal funcionamiento del software, etc.)

- Acciones no autorizadas (uso no autorizado de equipos, copia fraudulenta del software, uso de software falsificado o copiado, corrupción de datos, comportamientos no autorizados, procesamiento ilegal de datos, robo de información, etc.)

- Compromiso de las funciones (error en el uso, abuso de privilegios, suplantación de identidad, denegación de acciones, exposición de la disponibilidad del personal, etc.)

- No acceso a las instalaciones de la organización por parte de los funcionarios (huelga, manifestación pública, huelga de los sindicatos de la empresa, etc.)

**8.1.3 Controles del riesgo**

* **Responsabilidades y procedimientos:** Para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
* **Notificación de los eventos de seguridad de la información:** Se deber informar lo antes posible utilizando los canales de establecidos y adecuados.
* **Notificación de puntos débiles de la seguridad:** Informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.
* **Valoración de eventos de seguridad de la información y toma de decisiones:** Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.
* **Respuesta a los incidentes de seguridad:** Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.
* **Aprendizaje de los incidentes de seguridad de la información:** Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.
* **Recopilación de evidencias:** La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

**8.1.4 Métricas asociadas**

Número y gravedad de incidentes; evaluaciones de los costes de analizar, detener y reparar los incidentes y cualquier pérdida tangible o intangible producida.   
  
Porcentaje de incidentes de seguridad que han causado costes por encima de umbrales aceptables definidos por la dirección.   
  
Estadísticas del helpdesk de TI, con análisis sobre el número y tipos de llamadas relativas a seguridad de la información (p. ej., cambios de contraseña; porcentaje de preguntas acerca de riesgos y controles de seguridad de la información respecto al total de preguntas). A partir de las estadísticas, cree y publique una tabla de clasificación por departamentos (ajustada según el número de empleados por departamento), mostrando aquellos que están claramente concienciados con la seguridad, frente a los que no lo están.

**8.2 Auditorías internas y revisión por la dirección**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Los informes de auditoría interna del SGSI son la evidencia más directa que documenta los principales hallazgos, conclusiones y recomendaciones de la auditoría con la posibilidad de comunicar no conformidades y acciones correctivas, mejoras.   
  
Es necesario que los informes de auditoría atiendan a una programación de las auditorías en base a calendarios, presupuestos y asignaciones de días de trabajo del auditor, alcances de cada auditoría, archivos de documentos de trabajo de auditoria con hallazgos de auditoría detallados y evidencia (como listas de verificación completadas), recomendaciones de auditoría, planes de acción acordados y notas de cierre, etc.   
  
La imparcialidad y la competencia de los profesionales designados para auditar los requisitos del SGSI en el sector industrial de actividad de la organización y a sus sistemas de gestión de la información debe garantizarse.  
  
Los informes de revisión de la eficacia en la gestión del SGSI por parte de la dirección en base a una frecuencia predeterminada pueden verificarse mediante calendarios, presupuestos, alcances, documentos de trabajo con evidencia, recomendaciones, planes de acción, notas de cierre, etc. o cuestiones planteadas en los propios informes.

Las revisiones de seguimiento y las auditorías periódicas confirman que la organización sigue cumpliendo con la norma. El mantenimiento de la certificación requiere auditorías periódicas de reevaluación para confirmar que el SGSI continúa funcionando como se especifica y pretende. Al igual que con cualquier otra norma ISO, ISO/IEC 27001 sigue el ciclo PDCA y ayuda a la gestión del SGSI a conocer hasta qué punto y con qué éxito ha progresado la empresa a lo largo de este ciclo.

**8.3 No conformidades Acciones correctivas y preventivas**

Las no conformidades son requisitos del SGSI parcial o totalmente insatisfechos.  
El origen de los requisitos es obviamente el estándar ISO/IEC 27001 pero también surgen de las necesidades aplicadas por la propia organización (estrategias, políticas, procedimientos, pautas) o por partes externas a ella (leyes, regulaciones y contratos) en relación a las actividades del alcance del SGSI.  
  
Pueden documentarse en forma de problemas, eventos, incidentes, hallazgos de auditoría y revisión, quejas, o simplemente como "no conformidades" típicamente en formularios de no conformidad acción correctiva.   
  
Los auditores de certificación deben verificar que las no conformidades se identifican, investigan en sus causas de origen, informan, abordan y resuelven rutinaria y sistemáticamente.   
  
Mantener un registro o índice de no conformidades, junto con la evidencia cuidadosamente presentada de las acciones emprendidas en respuesta a las no conformidades, tales como:

* Reacción inmediata de contención o reparación de la no conformidad
* Análisis de causa raíz para evitar recurrencias
* Aplicación y resultados finales de la acción correctiva, incluida la revisión de su efectividad y finalización/cierre/aprobación de la no conformidad.

A continuación se muestra el formato de Conformidad:



|  |  |  |  |
| --- | --- | --- | --- |
| **6. CORRECTIVE/PREVENTIVE ACTION:** (Preventive action is only required for **potential non-conformities**). Fill ONLY EITHER “Corrective Action” OR “Preventive Action” | | | |
| Corrective Action: | | Preventive Action: | |
| Proposed by: | | Date: | |
| Proposed implementation date: | |
| **7. VERIFICATION OF VALIDITY OF CORRECTIVE “or” PREVENTIVE ACTION:** | | | |
| Addresses the root cause?  Prevents recurrence?  Valid  Invalid. Issue new NCPAR  Remarks: | | Addresses the root cause?  Prevents occurrence?  Valid  Invalid. Issue new NCPAR  Remarks: | |
| Signature:  (Lead Auditor) | Date: | Signature:  (Lead Auditor) | Date: |
| **8. FOLLOW-UP OF IMLEMENTATION CORRECTIVE/PREVENTIVE ACTION TAKEN:** | | | |
| Implementation of corrective action is:  🞎 Implemented  🞎 Not implemented. Issue new NCPAR  Remarks: | | Implementation of preventive action is:  🞎 Implemented  🞎 Not implemented. Issue new NCPAR  Remarks: | |
| Signature:  (Lead Auditor) | Date: | Signature:  (Lead Auditor) | Date: |
| **9. VERIFICATION OF EFFECTIVENESS OF IMPLEMENTED CORRECTIVE/PREVENTIVE ACTION:** | | | |
| Corrective action is:  🞎 Effective  🞎 Not effective. Issue new NCPAR  Remarks: | | Preventive Action:  🞎 Effective  🞎 Not effective. Issue new NCPAR  Remarks: | |
| Signature:  (Lead Auditor) | Date: | Signature:  (Lead Auditor) | Date: |

**ANEXO:**

**1. CRONOGRAMA DE IMPLEMENTACIÓN EXCEL**

**2. DECLARACIÓN DE APLICABILIDAD WORT**

**3. FORMATO DE CONTROL WORT**

**4. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN MEDPLUS+ WORT**