PLAN GENERAL DE SEGURIDAD DE LA INFORMACIÓN 2025

LIGIA ARIZA ALTAMAR

GERENTE

E.S.E CENTRO DE SALUD JOSÉ MARÍA FEREZ FARAH

Contenido

1. INTRODUCCIÓN

La información es el activo más importante y relevante para las organizaciones y recurso indispensable para el desarrollo y cumplimiento misional; ésta puede llegar a ser sensible o crítica y por lo tanto requiere de una evaluación para determinar su nivel de protección necesario para mitigar o evitar posibles situaciones de riesgo e impacto asociado a la pérdida de su disponibilidad, integridad o confidencialidad.

En atención a las situaciones de riesgo expuestas anteriormente, se genera en la E.S.E centro de salud José María Ferez Farah, la necesidad de seguir un modelo de gestión de la seguridad de la información que propenda por alcanzar y mantener una cultura y conciencia en el acceso y uso adecuado de la información en la entidad.

El presente documento identifica y recopila buenas prácticas para la gestión del ciclo de operación del modelo de seguridad y privacidad de la información, a partir de una evaluación de diagnóstico, planeación, implementación, gestión y mejora continua del mismo.

2. OBJETIVO

Presentar el plan de seguridad y privacidad de la información de la E.S.E. Centro de Salud José María Ferez Farah y los elementos que lo conforman, como marco de referencia para el establecimiento y regulación de lineamientos y medidas que permitan el aseguramiento de la protección y uso adecuado de la información y activos de información que la soportan al interior de la Entidad.

3. ALCANCE

El presente documento identifica e incluye las orientaciones para la gestión del ciclo de operación del modelo de seguridad y privacidad de la información, el cual debe ser aplicado sobre todos los procesos de la E.S. E y de cumplimiento por parte de todos los servidores públicos con relación contractual.

4. JUSTIFICACION

El presente plan de seguridad de la información se define en cumplimiento a sus propósito y obligaciones internos como sectoriales en cuanto a la contribución a la construcción de un estado más eficiente, transparente y participativo a través de la definición del MSPI, al igual que a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de Gobierno Digital.

5. PRESENTACION DE LA ENTIDAD

La ESE centro de salud de Usiacuri, basándose en los lineamientos de la Política Nacional de Prestación de Servicios de Salud, se compromete a brindar sus usuarios servicios de salud integrales de baja complejidad, con estándares superiores de calidad, orientados en criterios de mejoramiento continuo, humanización, atención segura para el paciente y su familia, enmarcados dentro de los

componentes del Sistema Obligatorio de Garantía de la Calidad, a través del desarrollo de programas y proyectos aportando al mejoramiento de la calidad de vida de la población.

6. CICLO DE OPERACIÓN DEL MSPI

En el 2025 se identificó la necesidad de definir las 5 fases que orientarían el ejercicio para los propósitos de protección de la información de la Entidad bajo un modelo sostenible; las fases del ciclo de operación se definen de la siguiente manera basadas en una fase inicial de diagnóstico:

6.1 FASE PREVIA DE DIAGNOSTICO DEL MSPI

En esta fase y mediante el uso de herramientas de diagnóstico, se desarrollaran en el 2025 y 2026 actividades de reconocimiento y valoración del estado de gestión, cumplimento de requisitos y lineamientos de seguridad de la información basado con el Modelo de Seguridad y Privacidad de Información de la estrategia de Gobierno Digital del Gobierno Nacional y de la implementación de controles de seguridad de la información con visión de mitigar todo tipo de escenario de riesgo asociado que pudiese generar un impacto indeseado a la Entidad.

El resultado de la evaluación de diagnóstico permitirá establecer en que ciclo de operación del modelo de seguridad y privacidad de la información MSPI se encuentra la E.S.E. centro de salud José María Ferez Farah y el mapa de ruta para las actividades claves de las fases de diseño y establecimiento del mismo modelo.

6.2 FASE DE PLANEACION

Para el desarrollo de esta fase y basado con el resultado de la evaluación de diagnóstico y el análisis de contexto, se identificaron los aspectos claves que definen y orientan las actividades para los propósitos de seguridad y privacidad de la información, entre ellos, la justificación, el alcance, la política y los objetivos del Modelo de Seguridad y Privacidad de la Información (MSPI).

6.2.1 Alcance del MSPI

El plan de seguridad y privacidad de la información y lineamientos asociados como directriz de la E.S.E continuaran con aplicabilidad e implementación para todos los procesos y aspectos administrativos de la organización y de cumplimiento por parte de todos aquellos servidores públicos y terceros que presten sus servicios o tengan algún tipo de relación con la Entidad.

El alcance del MSPI permitirá a la E.S.E. definir los límites sobre los cuales se implementará la seguridad y privacidad de la información, por tanto, deberá tener en cuenta, los procesos que impactan directamente la consecución de los objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados e interrelaciones del MSPI con otros procesos.

6.2.2 Gobierno de la seguridad y privacidad de la información

El modelo de gobierno de la seguridad de la información continuara a través de la estructura de directrices y lineamientos por niveles de acuerdo con el propósito de cada uno de ellos.

La estructura de directrices y lineamientos de seguridad de la información se define de la siguiente manera:

a. Política general de seguridad de la información: Documento de alto nivel que denota compromiso de la alta dirección con respecto a seguridad de la información; define reglas de comportamiento asociado a protección de activos de información.

b. Políticas Tácticas de seguridad de la información: Son exigencias particulares de apoyo a la política estratégica, manifiestan la manera en que se va a ejecutar a conseguir tienen propósito especial.

c. Normas y estándares de seguridad de la información: Todas aquellas reglas específicas orientadas para respaldar el cumplimiento de las políticas de gestión tecnológica.

Soporte Documental: Todo documento generado para dirigir y orientar la gestión de la seguridad de la información; permitirá compartir a los servidores públicos comprender los propósitos de seguridad de la información, las directrices y lineamientos relacionados con seguridad de la información.

Política General de Seguridad de la Información

Políticas Tácticas de SI

Políticas Operativas de SI (Normas y Estándares)

Toda la documentación asociada al sistema de gestión de seguridad de la información deberá ser revisada y actualizada (en la medida que aplique) bajo un estricto control de cambios para asegurar la integridad de los contenidos.

6.2.3 Política general de seguridad y privacidad de la información

La política de seguridad de información es la declaración general que representa por tal motivo define que:

La E.S. E Centro de Salud José María Ferez Farah continua reconociendo el valor de su información como uno de sus activos más valiosos y es consciente de la necesidad de su custodia, conservación, disponibilidad, integridad, accesibilidad y confidencialidad en los casos que corresponda, generando una cultura de protección y uso adecuado a través de la implementación y mejora continua de un sistema de gestión de seguridad de la información, con un enfoque de administración y tratamiento de riesgos asociados y el cumplimiento de todos los requisitos propios de su actividad, legales, reglamentarios y contractuales, que permitan asegurar la confianza de las partes interesadas.

6.2.4 Objetivos de seguridad y privacidad de la información

- ✓ Establecer las directrices y lineamientos relativos a seguridad de la información.
- ✓ Generar una cultura y apropiación de trabajo enfocada a la toma de conciencia para la protección y el uso adecuado de la información por parte de los servidores públicos.
- ✓ Implementar mecanismos de control para la protección de los datos, la información y los recursos asociados que los soportan.
- ✓ Asegurar que los riesgos asociados a seguridad de la información se mantienen en un nivel aceptable.
- ✓ Mantener un enfoque de cumplimiento estricto de los requisitos legales, normativos o contractuales aplicables y relativos al tratamiento y protección de la información.

6.2.5 Compromiso de la Alta Dirección

La gerencia a través de su equipo de trabajo este primer año genera el diagnostica para implementar la política general de seguridad de la información como muestra de su compromiso y apoyo a las actividades de diseño, implementación, mantenimiento y mejora continua de políticas y lineamientos consecuentemente orientados a la salvaguardar la confidencialidad, integridad y disponibilidad de la información de la Entidad.

Su compromiso se demostró a través de:

- ✓ En el primer año realizara el diagnóstico de la implementación inicial de la política y lineamientos de seguridad de la información.
- ✓ La promoción de una cultura de seguridad y protección de la información.
- ✓ El apoyo para la divulgación de los propósitos y lineamientos de seguridad de la información a los servidores públicos y partes interesadas.
- ✓ La asignación de los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información.
- ✓ La realización de actividades de verificación y evaluación del desempeño del sistema de gestión de seguridad de la información de manera periódica.

6.2.6 Roles y Responsabilidades de MSPI

La E.S.E. Centro de Salud José María Ferez Farah definió una estructura de roles y asignación formal de responsabilidades orientados a la seguridad y privacidad de la información en diferentes niveles de la Entidad para permitir la adecuada y oportuna toma de decisiones enfocados al cumplimiento de los objetivos de seguridad y privacidad de la información (MSPI) de la Entidad.

A quien está dirigido el MSPI:

Líderes de áreas y de procesos, entendiendo los propósitos de la Entidad y a los cuales deberán prestar su apoyo y responsabilidad para su aplicación.

Grupos Internos de Trabajo, tales como Control Interno, Talento Humano, coordinación científica y demás áreas operativas de la E.S.E , para promover y aplicar las políticas, estándares y demás lineamientos del manual de seguridad de la información.

Terceras partes, tales como entidades descentralizadas, y entidades de regulación, quienes requieren de su consulta para la comprensión de la estructura y conformación de la seguridad de la información, en beneficio del cumplimiento de las obligaciones legales, contractuales y demás aplicables.

Todos los funcionarios, contratistas, o partes interesadas, que presten sus servicios o tengan algún tipo de relación con la Entidad, quienes deben ser informados de las responsabilidades de seguridad a través de los términos y condiciones o contratos laborales, procedimientos de seguridad y guías, entrenamiento y sensibilización.

6.2.7 Plan de Comunicaciones

La E.S.E. identificara y aplicara el plan de comunicaciones, de sensibilización y de capacitación que promueva estrategias para crear, incentivar y mantener una cultura organizacional mediante la generación de competencias y hábitos de protección de la información en todos los niveles de la Entidad.

El plan de comunicaciones de seguridad y privacidad de la información, y especialmente con respecto a actividades de socialización y sensibilización dirigida a los servidores públicos continuara siendo ejecutado en conjunto con el apoyo del área de comunicaciones de la E.S.E. Centro de Salud José María Ferez Farah

6.3 FASE DE IMPLEMENTACION

El desarrollo de estas fases va después del proceso de diagnóstico y la planeación la cual permitirá a la E.S.E. llevar a cabo la implementación de los aspectos y planes identificados en las fases anteriores

Un plan de control operacional establecerá las actividades y la programación para la implementación tanto de los requisitos, controles y buenas prácticas de seguridad y privacidad de la información en la E.S.E. Centro de Salud José María Ferez Farah.

Como estrategia para la orientación de los propósitos de seguridad y privacidad de la información al interior de la E.S.E. Centro de Salud José María Ferez Farah , se definen y aprueban políticas y directrices que guiarán las prácticas de protección de la información en cuanto a su confidencialidad, integridad y disponibilidad.

7. POLITICAS Y DIRECTRICES DE SEGURIDAD DE LA INFORMACION

Lineamientos que describen los principios de seguridad y privacidad de la información definidos y ajustados a las necesidades de la E.S.E., en orientación de los propósitos asociados a la protección de la confidencialidad, integridad y disponibilidad de la información y activos que la soportan.

7.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

En la E.S.E. Centro de Salud José María Ferez Farah liderara la gestión de seguridad de la información a través de la identificación de una estructura de roles y responsabilidades, que involucren las actividades de direccionamiento, implementación y control operacional en beneficio del cumplimiento de los propósitos de protección de la información y su mantenimiento eficaz a través del tiempo, así como de la conformación y asignación de responsabilidades pertinentes al sistema de gestión de seguridad de la información de la Entidad.

7.1.1 Uso de dispositivos móviles

Teniendo en cuenta el alto grado de exposición que representa la información y los datos la E.S.E. Centro de Salud José María Ferez Faraha través del acceso y uso de dispositivos móviles de propiedad de terceros (teléfonos móviles, tabletas, portátiles, medios de almacenamiento USB);La E.S.E establece directrices de uso y manejo de equipo portátil y dispositivos móviles:

La E.S.E. Centro de Salud José María Ferez Farah autoriza el uso de dispositivos móviles para el acceso y uso a la información y datos de la Entidad, siempre y cuando, exista una relación contractual entre las partes y éstos sean utilizados para el apoyo al cumplimiento de sus responsabilidades y de los objetivos contractuales.

Los usuarios de dispositivos móviles no estarán autorizados a cambiar la configuración de dispositivos móviles de propiedad de la E.S.E. , a desinstalar software, formatear o restaurar configuraciones de fábrica; únicamente se deberá aceptar y aplicar actualizaciones.

7.1.2 Seguridad de la Información en proyectos

Los proyectos en la E.S.E. Centro de Salud José María Ferez Farah deberán considerar la relevancia de su información durante las diferentes etapas de estos, con el propósito de otorgar la protección necesaria basada en la identificación y valoración de los riesgos asociados a la pérdida de la confidencialidad, disponibilidad e integridad de la información.

7.2 POLITICA DE SEGURIDAD DE RECURSOS HUMANOS.

La E.S.E. Centro de Salud José María Ferez Farah continuará promulgando la aplicación de criterios de control de seguridad de los recursos humanos en los procesos de contratación de personal, que permitan asegurar la idoneidad de los candidatos basada en la responsabilidad y ética pertinentes de acuerdo con las necesidades de los roles a ocupar y la clasificación de la información a la cual accederá.

La E.S.E. Centro de Salud José María Ferez Farah continuara divulgando con periodicidad definida, las directrices y lineamientos de seguridad de la información a todos los servidores públicos o terceros que tenga una relación contractual con la Entidad o que tengan acceso a la información de la Entidad, de manera que, se entiendan y comprendan sus responsabilidades y obligaciones asociadas, bien como usuarios o con la responsabilidad compartida desde los roles asignados.

Se deberá capacitar y sensibilizar a los colaboradores de la E.S.E. y terceros con respecto a los propósitos de la protección de la información en la Entidad.

La E.S.E. Centro de Salud José María Ferez Farah se asegurará acerca de la aceptación de las responsabilidades del acceso y uso de información o activos de información en aseguramiento de la confidencialidad de la información y transparencia mediante la firma de formato definido por la Entidad.

Todos los colaboradores de la E.S.E. o terceros deberán realizar la devolución de cada uno de los activos de información asignados, ante la terminación del contrato acordado.

Funcionarios, contratistas, terceros o cualquier persona que tenga una relación contractual o laboral con la Entidad, o que tenga acceso a los activos de información de La E.S.E. Centro de Salud José María Ferez Farah, deberán mantener la confidencialidad de la información de su acceso y conocimiento dentro o fuera de las instalaciones de la Entidad.

7.2.1 Gestión de Activos de Información

Todos aquellos activos de información la E.S.E. Centro de Salud José María Ferez Farah incluida la información que sean sensibles o críticos para la operación o cumplimiento de la misión de la Entidad, deberán contar con la asignación de protección de su confidencialidad, integridad y disponibilidad en concordancia con los resultados de una evaluación de riesgos y el nivel de exposición identificado.

Activos de información de los procesos de La E.S.E. Centro de Salud José María Ferez Farah deberán ser identificados y administrados dentro de un inventario, al igual que valorados con respecto a su

sensibilidad o criticidad frente a impactos de afectación sobre la confidencialidad, integridad y disponibilidad de estos.

7.2.2 Acceso y Uso de información

Todo funcionario, colaborador o persona entenderá y asumirá su responsabilidad de protección de la información a través de su acceso y uso apropiados.

La E.S.E. Centro de Salud José María Ferez Farah será el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los servidores públicos o terceros, derivados del objeto y en cumplimiento de las funciones o tareas asignadas bajo acuerdo contractual.

Todos los colaboradores de la E.S.E. o terceros deberán firmar el acuerdo de confidencialidad y transparencia, en el cual se establece la responsabilidad de confidencialidad de la información de la Entidad bajo su responsabilidad.

Todo colaborador o tercero previo a recibir su cuenta de acceso a los sistemas de información de la E.S.E. , deberá firmar y aceptar una declaración de responsabilidad sobre el uso y acciones realizadas con dichas cuentas.

Los usuarios no deberán almacenar información en discos duros de los equipos de cómputo o virtuales disponibles, archivos de video, música, fotos o cualquier tipo de archivo que no sea de carácter institucional.

7.2.3 Clasificación de la Información

Toda información al interior de La E.S.E. Centro de Salud José María Ferez Farah deberá recibir el nivel de clasificación apropiado de acuerdo con las necesidades de protección de la misma y a los riesgos potenciales asociados

Toda Información clasificada deberá recibir el sistema de etiquetado con la identificación del nivel de clasificación asignado.

7.2.4 Manejo disposición de información, medios y equipos

Se establecerán controles para evitar la divulgación, modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados, velando por la disponibilidad y confidencialidad de la información.

Los medios y equipos donde se almacena la información deberán mantenerse con las medidas de protección físicas y lógicas aplicables, se deberán generar los planes de mantenimientos preventivos y correctivos que se requieran.

Para el retiro de equipos de cómputo por su estado de obsolescencia y/o daño, se deberá garantizar la aplicación del procedimiento de saneamiento, es decir llevar a cabo buenas prácticas para la eliminación y/o destrucción de la información con herramientas automáticas que aseguren que la misma no pueda en ningún caso ser recuperada.

Toda aquella información que por su obsolescencia se encuentre en medio físico papel y ésta no sea confidencial, deberá ser eliminada mediante la técnica de rasgado o picado mediante el uso de equipo especializado.

7.2.5 Uso y protección de equipo de cómputo

En equipo de cómputo de propiedad de la E.S.E. únicamente se podrá instalar y utilizar software o programas, sistemas de información, herramientas de software en equipos de cómputo de propiedad de La E.S.E. Centro de Salud José María Ferez Farah que sean licenciados y autorizados por la E.S.E.

Equipo de cómputo no podrán ser utilizados para actividades de divulgación, propagación o almacenamiento de contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso, o cualquier otro uso que no esté autorizado.

7.2.6 Uso de Correo Electrónico

La E.S.E. Centro de Salud José María Ferez Farah tendrá el derecho a realizar monitoreo o seguimiento del uso del correo electrónico a todos funcionarios y/o contratistas a quienes se les conceda una cuenta de correo corporativa.

Usuarios no deberán participar en correo electrónico que incite o incentive el envío de cadenas o publicidad que no sean interés o estén relacionados con La E.S.E. Centro de Salud José María Ferez Farah.

No se deberán realizar el envío o distribución de información catalogada como confidencial, interna o privada dentro o fuera de la E.S.E. Centro de Salud José María Ferez Farah (sin la autorización correspondiente).

No se podrá hacer uso de lenguaje ofensivo, inapropiado o con declaraciones de blasfemia, obscenidad, ilegales, incitadores a infringir la ley, hostigamiento basado en sexo, raza, nacionalidad, contenido despectivo o difamatorio en cualquier mensaje electrónico para con sus compañeros, clientes, proveedores u otros; su uso inadecuado, se considerará fuera del alcance y responsabilidad la E.S.E. Centro de Salud José María Ferez Farah por lo tanto, los daños y perjuicios que pueda llegar a causar, serán de completa responsabilidad de Se prohíbe el envío de correos masivos al interior de la organización; sólo los usuarios autorizados por la gerencia y los jefes de área podrán enviar dichos correos.

Está prohibido utilizar el correo electrónico para el intercambio de información o de software que violen las leyes de derechos de autor.

Es responsabilidad de los usuarios de correo electrónico hacer mantenimiento a su buzón de correo: eliminar mensajes de la bandeja de entrada, archivar mensajes, Eliminar definitivamente los mensajes de la bandeja Elementos Eliminados.

Se debe ingresar al correo electrónico institucional por la página web https://hospitaldeusiacuri.co única y exclusivamente.

7.2.7 Uso de Impresora y servicio de impresión

Los documentos que se impriman en las impresoras de La E.S.E. Centro de Salud José María Ferez Farah deberán ser de carácter institucional.

Labores de reparación o mantenimiento de las impresoras es exclusivo de ejecución por parte de la persona contratada para ello y ningún funcionario o persona podrá realizar dicha actividad.

Puertos de salida USB de las impresoras deberán ser bloqueadas o restringidos para su uso en beneficio de prevención de la fuga de información.

7.2.8 Escritorio y Pantalla limpias

Los escritorios (puestos de trabajo) deberán estar en la medida de lo posible organizados y libres de la exposición de información documental que sea clasificada como confidencial.

Las pantallas de equipos de usuarios deberán ser bloqueadas para aquellos momentos en que no esté utilizando el equipo o ante la ausencia del funcionario de su puesto de trabajo.

Se deberá utilizar de fondo de pantalla de los equipos de cómputo de propiedad de La E.S.E. Centro de Salud José María Ferez Farah el indicado por la alta dirección única y exclusivamente.

7.2.9 Uso de Internet

Se reserva el derecho de realizar monitoreo o seguimiento de los accesos a sitios en internet realizados por parte de los funcionarios.

Se permitirá el acceso a servicios de internet, con lineamientos que garanticen la navegación y uso controlados de componentes del servicio.

Se restringirá toda posibilidad de descarga de software no autorizado o código malicioso en los equipos de cómputo de la E.S.E a través de internet, así mismo.

El acceso y uso del servicio de internet se concederá solo para propósitos laborales o fines particulares definidos y aprobados por la E.S.E.

Para los propósitos de almacenamiento de archivos e información, se debe realizar en la nube Drive, al igual que se debe solicitar un espacio en los discos duros de la entidad y en el servidor para realizar las copias.

Se restringirá el acceso a sitios web dedicados a compartir material audiovisual fotos, videos, streaming tales como Facebook, Youtube, Flickr, etc, solamente podrán acceder a ellos la persona encargada de las comunicaciones y redes sociales de la entidad.

No se permitirá el acceso a sitios web con contenidos que están en contra de la ley, principios de ética moral de La E.S.E. Centro de Salud José María Ferez Farah tales como, pornografía, terrorismo, contenidos obscenos, discriminación racial o similar.

7.3 POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL

La E.S.E. Centro de Salud José María Ferez Farah definirá y aplicará protocolos de control de acceso a las instalaciones y áreas especiales que requieran de un mayor nivel de seguridad física, en beneficio de resguardar la confidencialidad e integridad de personas, información y activos de información en general.

Áreas determinadas seguras para la E.S.E. tales como centro de datos, cuartos de cableado, archivo documental, entre otras, deberán recibir, el control de acceso restringido de personal, mantener un

registro de ingreso y control mediante vigilancia de cámaras del acceso de personal autorizado como visitantes autorizados en áreas seguras, la instalación y mantenimiento de controles de seguridad ambiental a modo de mitigar situaciones de impacto no deseados.

Se deberán definir e implementar programas de mantenimiento preventivo y correctivo de los equipos de cómputo instalados en las áreas seguras de la E.S.E.

7.4 POLÍTICA DE GESTIÓN DE CONTROL DE ACCESO

La E.S.E. Centro de Salud José María Ferez Farah definirá las pautas y criterios generales para controlar y asegurar la asignación de derechos de acceso lógico a usuarios sobre los sistemas operativos, datos o información, servicios de información de la plataforma tecnológica o red de datos que sea concedida.

Toda asignación de derechos de acceso lógico a usuarios se realizará bajo el cumplimiento de un protocolo y diligenciamiento de solicitud y autorización formales.

Contraseñas de usuarios de acceso a información o servicios de red deberán mantenerse confidenciales bajo buenas prácticas de protección de confidencialidad de estas.

El control de acceso a los equipos de cómputo deberá realizarse a través de un servicio de Directorio Activo, que permita su autenticación, validación y autorización confiables.

7.5 POLÍTICA DE GESTIÓN DE OPERACIONES Y COMUNICACIONES

Procedimientos de gestión tecnológica asociados a la administración de equipo crítico tales como servidores, deberán ser documentados de manera clara y con información actualizada si excepción alguna.

La E.S.E. Centro de Salud José María Ferez Farah definirá e implementará estrategias y mecanismos de control sobre la operación tecnológica, redes de datos y todo aquel sistema de comunicación, que permita asegurar y mantener la disponibilidad de componentes, herramientas y servicios tecnológicos esenciales para la operación de la Entidad.

Directrices de uso de la seguridad de la información deberán ser definidas para la prestación de los servicios tecnológicos con enfoque de protección de la información y de los equipos de cómputo, asegurando continuidad en los servicios tecnológicos.

Se deberá establecer proyección de capacidad futura de componer Información tanto crítica como sensible de la E.S.E. deberá ser respaldada y custodiada de manera segura, siguiendo el procedimiento establecido.

Procedimientos e instructivos para la toma de respaldo y recuperación de información deberán ser documentados; de igual manera, se deberá identificar los tiempos de retención de los medios donde se almacena la información de respaldo.

Toda conexión inalámbrica deberá ser establecida bajo las condiciones y medidas de seguridad basadas en la configuración y el monitoreo de las redes locales inalámbricas y de los dispositivos allí conectados para la conexión a dichas redes.

Todos los dispositivos de la infraestructura de conectividad inalámbrica en La E.S.E. Centro de Salud José María Ferez Farah deberán cumplir con lineamientos y estándares definidos para tal fin.

7.6 POLITICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

Se deberán estructurar pautas y lineamientos de control de seguridad de la información para las actividades de adquisición, desarrollo y mantenimiento de los sistemas de información de La E.S.E. Centro de Salud José María Ferez Farah, para las cuales se promulgue la confidencialidad, integridad y disponibilidad como parte integral de los mismos.

El proceso de adquisición y desarrollo de las aplicaciones debe ser estructurado y ordenado, considerando las diferentes etapas del ciclo de vida de las soluciones. La documentación de cada uno de los sistemas implantados en la E.S.E. debe contener la guía para brindar soporte, la cual incluya copia del contrato con el proveedor que lo brinda, en caso de que aplique esta modalidad, especificando los Acuerdos de Nivel de Servicio (ANS) establecidos, los interlocutores y los procedimientos para obtener el servicio.

7.7 POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La E.S.E. Centro de Salud José María Ferez Farah asegurará que tanto los eventos como los incidentes de seguridad de la información sean registrados, analizados y atendidos de manera oportuna, bajo la definición de un protocolo establecido, el cual oriente en las actividades a realizar y en la toma de decisiones oportunas para una mitigación o reducción de impactos indeseados sobre la Entidad.

7.8 POLITICA DE GESTION DE PROVEEDORES

La E.S.E. Centro de Salud José María Ferez Farah identificará pautas para establecer y mantener relaciones claras y fortalecidas con aquellos terceros con quien se establezca una relación contractual bien sea de servicios o de productos, que aseguren el adecuado cumplimiento de los acuerdos establecidos, donde se garantice la aplicación de medidas de seguridad de la información en cumplimiento de los objetivos de la Entidad.

7.9 POLÍTICA DE GESTIÓN DE SEGURIDAD EN LA CONTINUIDAD DEL NEGOCIO

La Entidad identificará las necesidades y requisitos de seguridad de la información para su vinculación en el plan de continuidad de negocio, de modo que se asegure que, ante situaciones de crisis o desastres, no se descuide los niveles de seguridad y se incurra en impactos indeseados.

7.10 POLÍTICA DE GESTIÓN DE CUMPLIMIENTO

La E.S.E. Centro de Salud José María Ferez Farah mantendrá estrategias para la identificación y actualización de información acerca de legislación, normatividad o regulación nacional relacionada con la protección de datos y/o seguridad de la información para las cuales se deba enfocar estricto cumplimiento.

La E.S.E. Centro de Salud José María Ferez Farah mantendrá el inventario y actividades de actualización de toda aquella legislación o regulación nacional relacionada con la protección de datos y/o seguridad de la información para las cuales se deba enfocar estricto cumplimiento.

7.10.1 Política de Incorporación al Cumplimiento Regulatorio

Toda solución de servicios o infraestructura tecnológica debe cumplir con las condiciones contractuales, de legislación y regulación externa o interna, para el debido cumplimiento de los regímenes legales a los cuales está sometido a La E.S.E. Centro de Salud José María Ferez Farah.

8. EVALUACION DEL DESEMPEÑO DEL MSPI

Con el propósito de conocer los estados de cumplimiento de los objetivos de seguridad de la información, se mantendrán esquemas de seguimiento y medición al cumplimiento de aspectos del modelo de seguridad y privacidad de información que permitan contextualizar una toma de decisiones de manera oportuna.

8.1.1 Seguimiento y Medición

Para las actividades de seguimiento y medición, La E.S.E. Centro de Salud José María Ferez Farah definirá los procedimientos que permitan:

- ✓ Definir y orientar actividades para la identificación de situaciones de eventos o incidentes de seguridad y privacidad de la información.
- ✓ Definir los esquemas de atención a los eventos e incidentes de seguridad de la información, en beneficio de prevenir y mitigar escenarios de impacto a la Entidad.
- ✓ Emprender revisiones regulares de la eficacia del MSPI (que incluyen el cumplir de la política de seguridad de la información, los objetivos, los controles) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugeridas y la retroalimentación de las partes interesadas.
- ✓ Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.
- ✓ Revisar las valoraciones de riesgos de manera regular, asegurando que los niveles de riesgos residuales son comprendidos y aceptados.
- ✓ Realizar actividades de revisión del MSPI por parte de la Alta Dirección de la E.S.E.

9. MANTENIMIENTO Y MEJORA DEL MSPI

La Entidad con la visión de mantenimiento y mejora de los aspectos de seguridad de la información, tomará en cuenta los resultados de la fase anterior “Evaluación de desempeño” basada en los resultados de las actividades de seguimientos y medición (indicadores).

La E.S.E:

- ✓ Implementará las mejoras identificadas en el MSPI
- ✓ Identificará e implementará acciones correctivas y preventivas que mitiguen situaciones de impacto.

- ✓ Implementará acciones de mejora basadas en las lecciones aprendidas de las experiencias de seguridad internas o de otras entidades.
- ✓ Asegurar que las mejoras cumplen con los objetivos y propósitos definidos por la E.S.E.

10 CRONOGRAMA MSPI

La Entidad definirá y mantendrá un cronograma de actividades en cumplimiento a los propósitos internos de seguridad y privacidad de la información basada en el ciclo de operación MSPI.

LIGIA ARIZA ALTAMAR

GERENTE