PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
VIGENCIA DEL PLAN 2020-2024
AJUSTE VIGENCIA 2021

Implementado por
Ingeniero YOJAN NARVAEZ
OFICINA DE SISTEMAS DE INFORMACION Y COMUNICACIÓNES

Elaborado por
MARIXA BAYONA BARRERO
ASESOR DESARROLLO ORGANIZACIONAL

JARQUIN EBERTO MELENDEZ BARON
GERENTE ESE CAMU DEL PRADO DE CERETE

Cereté, enero 26 de 2021

CONTENIDO

10.LISTADO DE DOCUMENTOS CONFIDENCIALES

1. INTRODUCCIÓN

La ESE CAMU DEL PRADO DE CERETE - Córdoba en busca de la mejora continua implementar un método lógico y sistemático que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados el manejo de la información institucional, para lograr que estos no afecten de una manera relevante a la misma.

La institución en su quehacer diario utiliza TIC en cuanto a captura, procesamiento y reporte de información tanto internamente como externamente para comunicarse con los diferentes actores del sistema de salud, lo cual implica que la institución sea vulnerable a ataques mal intencionados o mala manipulación de la información lo que acarrea problemas económicos, legales, y administrativos por lo cual este documento busca establecer un línea de trabajo que permita a la entidad sortear los riesgos que lo rodean y lograr que su información este segura.

2. OBJETIVOS

2.1 Objetivo general

Desarrollar un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información el cual sea una guía para el control y minimización de los riesgos y así proteger la privacidad de la información y los datos tanto de los procesos como de las personas vinculadas con la información de la institución.

2.2 Objetivos Específicos

- Lograr un diagnóstico real de la situación actual de la institución

en materia de riesgos de seguridad y privacidad de la Información

- Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la función pública y Mintic para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información

- Optimización de los recursos de la institución en la aplicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

3. ALCANCE

El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional de manera transversal.

4. MARCO CONCEPTUAL

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberespacio: Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua española). Control Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Gestión de incidentes de seguridad de la información Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Parte interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

5. MARCO NORMATIVO

- Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública
- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública
- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales
- Ley 594 de 2000 - Ley General de Archivos
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del

Sector de Tecnologías de la Información y las Comunicaciones

- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos
- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública
- Decreto 2364 de 2012 - Firma electrónica
- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos
- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales
- Ley 527 de 1999 - Ley de Comercio Electrónico
- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley Estatutaria 1581 de 2012 - Protección de datos personales
- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información
- Decreto 103 de 2015, reglamenta parcialmente la Ley 1712 de 2014

6. DESCRIPCIÓN DEL PLAN

6.1 Identificación del riesgo

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas recolectan datos de entrada para esta actividad.

Normalmente se identifican los riesgos como eventos o situaciones no deseadas que se pretenden evitar, por tal razón la identificación de riesgos inicia con términos como: Ausencia, No adherencia, Inadecuada, No suficiencia, entre otros.
Una vez se identifique el riesgo, debe complementarse para obtener el contexto del riesgo, ya que éste puede presentarse en un área, en un horario, por parte de un grupo de colaboradores, o en unas circunstancias específicas que ayudarán más adelante a determinar las acciones a tomar. Estos son algunos ejemplos de preposiciones a utilizar: al, durante, en, sobre, con, hacia, de, mediante, entre otros.

6.2 Categorías de riesgos

ET: Estratégicos: Relacionados a lineamientos, políticas, estrategias o directrices no adecuadas o no convenientes para la Entidad.

OP: Operativo: Relacionado a procesos, conductas o actividades inapropiadas, contrarias al deber ser o que presente una posible brecha frente a la calidad esperada.

FA: Financiero: Relacionado con la asignación, suficiencia o recaudo de recursos económicos que puedan afectar a corto, mediano o largo plazo financieramente a los procesos o la entidad.

TEC: Tecnológico: Relacionado al uso, manejo o disposición de equipos biomédicos, industriales o de cómputo y periféricos.

CL: Clínico: Relacionados a condiciones patológicas de pacientes atendidos en el CAMU DE MOÑITOS, considerar la aplicación de la metodología AMFE según lo definido en el MP-0266 MANUAL DE GESTION INTEGRAL DEL RIESGO.

6.3 Descripción de Causas:

Se describen las causas asociadas al riesgo identificado, pueden ser intrínsecas: atribuidas a personas, métodos, materiales, equipos, instalaciones, directamente involucradas en el proceso o externas: cuando provienen del entorno en el que se desarrolla el proceso.

6.4 Consecuencias

Se describen los efectos asociados a la materialización del riesgo, que incidan sobre el objetivo del proceso o la Entidad. Pueden agruparse en: Daños a pacientes o trabajadores, Pérdidas económicas, Perjuicio de la imagen, Sanciones legales, reproceso, Demoras, Insatisfacción, entre otras.

6.5 Barreras de Seguridad Existentes

Se describen los controles implementados o barreras que existen actualmente para evitar la materialización del riesgo, se pueden encontrar en los protocolos o procedimientos documentados, en las

guías de reacción inmediata o en los correctos de buenas prácticas de seguridad del paciente.

6.6 Valoración del Riesgo:

Se mide en cuanto a probabilidad e impacto para obtener un dato cuantitativo que permita su comparación y priorización, como se muestra en las siguientes escalas de valoración:

Ver figura siguiente hoja

PROBABILIDAD		
Remota	1	La probabilidad de ocurrencia es muy baja, casi nula
Poco Probable	2	Puede ocurrir bajo circunstancias excepcionales
Probable	3	Puede ocurrir con cierta frecuencia
Ocasional	4	Ocurre algunas veces
Frecuente	5	La ocurrencia se da de manera común en circunstancias actuales

IMPACTO		
Muy bajo	1	Los efectos de materialización del riesgo no son significativos
Bajo	2	Los efectos de materialización del riesgo son poco significativos
Moderado	3	Los efectos de materialización del riesgo pueden significar aspectos moderados
Alto	4	Los efectos de materialización del riesgo son significativos e importantes
Muy Alto	5	Los efectos son catastróficos, como muerte, lesiones incapacitantes o liquidación de la empresa

	5	5	10	1	2	2
	4	4	8	1	1	2
	3	3	6	9	1	1
	2	2	4	6	8	1
	1	1	2	3	4	5
		1	2	3	4	5
		IMPACTO				

NIVEL	DE MEDIDAS DE RESPUESTA
BAJA	ASUMIR EL RIESGO Y CONTINUAR MONITORIZANDOLO
ACEPTABLE	REDUCIR EL RIESGO PARA LLEVARLO A ZONA BAJA
ALTA	EVITAR-COMPARTIR-TRANSFERIR POR MEDIO DE UN PLAN DOCUMENTADO
INACEPTABLE	EVITAR-COMPARTIR-TRANSFERIR POR MEDIO DE UN PLAN DOCUMENTADO

Figura 1.- Medición del riesgo impacto y probabilidad. **Fuente**: elaboración propia

6.7 Tratamiento y Seguimiento del Riesgo:

Se describen los controles o barreras a ser implementadas que fortalezcan las existes, con lo cual aportar y evitar la materialización del riesgo desde la reducción de la probabilidad y/o del impacto. Las acciones propuestas pueden en algunos casos significar actualización de protocolos o procedimientos documentados, adopción de mejores prácticas a través de referenciaciones realizas, fortalecimiento de buenas prácticas de seguridad del paciente, asesorías con expertos, entre otras.

Un aspecto de gran importancia es la definición de indicadores para determinar el impacto de las acciones realizadas, ya que no es suficiente cumplir las actividades propuestas sino también valorar como estas acciones permiten disminuir la probabilidad de ocurrencia o nivel de impacto del riesgo; es decir, el indicador mide la efectividad de las acciones frente a la mitigación del riesgo.

El sector público pensando en adaptarse con facilidad y seguridad a las necesidades de la ciudadanía, diseño la estrategia de gobierno en línea en donde se contempla la seguridad y privacidad de los datos que hacen parte del sector público y de la ciudadanía. Buscando garantizar un gobierno más operativo, eficiente, transparente y seguro para los ciudadanos. La estrategia de gobierno en línea del sector público colombiano tiene bases de la norma ISO/IEC 27001/2013, donde ofrece a las entidades del Estado asegurar la información y velar por su privacidad, mediante esquemas de sistemas de gestión de seguridad de la información, fortaleciendo las (TIC) en todas las entidades del estado que implementen la estrategia.

7. CONTROLES A IMPLEMENTAR EN EL PLAN DE SEGURIDAD

Fundamentados en el anexo A del estándar ISO/IEC 27001 y dominios a los que pertenece:

Nro.	NOMBRE	DESCRIPCION/JUSTIFICACION
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACION	Control: Definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes
		Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
A.6.1	Organización interna	Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización
A.6.1.1	Roles y responsabilidades para la seguridad de información	Control: Definir y asignar mediante notificación o circular, todas las responsabilidades de la seguridad de la información
A.6.2	Dispositivos móviles y teletrabajo	Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
A.6.2.1.	Política para dispositivos móviles	Control: Adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.1	Teletrabajo	Control: Implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7	Seguridad de los recursos humanos	
A.7.1	Antes de asumir el empleo	Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
A.7.1.1	Selección Control:	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los

		requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información
A.7.2	Durante la ejecución del empleo	Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
A.7.2.1	Responsabilidades de la dirección	Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3	Proceso disciplinario	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información
A.8	Gestión de activos	
A.8.1	Responsabilidad por los activos	Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas
A.8.1.1	Inventario de activos	Control: identificar los activos asociados con la información y las instalaciones de procesamiento de información, Elaborar y mantener un inventario de estos activos y de la arquitectura institucional
A.8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deberían tener un propietario, es decir asignar el responsable del mismo.
A.8.1.3	Uso aceptable de los activos	Control: Identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al

		terminar su empleo, contrato o acuerdo
A.8.2	Clasificación de la información	Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
A.8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.12.4	Registro y seguimiento	Objetivo: Registrar eventos y generar evidencia
A.12.4.1	Registro de eventos	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
A.14	Adquisición, desarrollo y mantenimientos de sistemas	
A.14.1.1	Requisitos de seguridad de los sistemas de información	Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.
A.14.2	Seguridad en los procesos de desarrollo y soporte	Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

Fuente: Norma técnica

8. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad, por sus siglas en ingles Statement of Applicability (SoA), es un elemento fundamental para la implementación del Modelo de Seguridad y Privacidad de la Información.

- La declaración de aplicabilidad se debe realizar luego del tratamiento de riesgos, y a su vez es la actividad posterior a la evaluación de riesgos.

- La declaración de aplicabilidad debe indicar si los objetivos de control y los controles se encuentran implementados y en operación, los que se hayan descartado, de igual manera se debe justificar por qué algunas medidas han sido excluidas (las innecesarias y la razón del por qué no son requeridas por la Entidad). Dentro de las actividades a seguir, después de la selección de los controles de seguridad, se procede a crear el plan de tratamiento de riesgos, esto con la finalidad de definir las actividades necesarias para la aplicación de los controles de seguridad.

9. DECLARACION DE SEGURIDAD DE LA INFORMACION

Trabajamos diariamente con pasión, respeto, transparencia y confianza, para mejorar la calidad de vida de nuestros usuarios a través de una experiencia única, sostenible y con estándares de garantía de la calidad en su portafolios institucional y prestación de servicios. Nuestra Estrategia de Sostenibilidad y Modelo de atención, basada en los principios de moralidad del sector público y transparencia en el acceso de la información, busca conducir a las diferentes dependencias hacia la transformación de la empresa en un sistema operacional sostenible.

Conscientes de esto, es que surge la "Declaración de Seguridad de la información", que tiene por objetivo brindar un resumen de los controles y procesos de seguridad dentro de la Empresa. Este documento es para uso con terceros (usuarios, proveedores, clientes internos) que estén relacionados o comprometidos con la ESE, y que deseen conocer sobre los arreglos de seguridad dentro del grupo. Esta declaración será revisada y actualizada anualmente.

9.1. Compromiso con la Seguridad

Está comprometido con mantener y mejorar continuamente la seguridad para cumplir con nuestras responsabilidades, con nuestros usuarios y organismos reguladores, para reducir exposición a riesgos, sanciones legales, pérdidas operativas o daños a la reputación. Como empresa, nos comprometemos con:

· La confidencialidad de la información corporativa, de usuarios, proveedores y de clientes

· La integridad de la información

· La disponibilidad de nuestra información

· El cumplimiento de requisitos legales, regulatorios y reglamentarios

· Brindar capacitación en seguridad de la información y conciencia de riesgos a todo el personal

· Informar e investigar violaciones de la seguridad de la información, reales o sospechas.

9.2 Organización de Riesgos de Información y Ciberseguridad

La administración de la ESE en su conjunto, es responsable de identificar, evaluar y administrar el espectro de riesgos a los que está expuesto la entidad. La ESE aplica un modelo de protección que garantiza que los riesgos y controles sean gestionados adecuadamente dentro de sus unidades de negocios o áreas, funciones y equipos de tecnología, de manera continua.

9.3 Estructura de Gobernanza de Seguridad de la información / Ciberseguridad

- Nombre: JOHAN SEBASTIAN NARVAEZ
- Cargo: RESPONSABLE OFICINA DE SISTEMAS DE INFORMACION Y COMUNICACIONES

9.4 Personal ESE CAMU DEL PRADO DE CERETE

En la ESE, la revisión de antecedentes es una defensa clave a nivel grupo contra el uso de información privilegiada y otros riesgos y se han definido requisitos mínimos de antecedentes. Todos los colaboradores del grupo ESE, incluyendo contratistas, proveedores de servicios y trabajadores de contingencia son sujetos a revisión de antecedentes, previo a entrar a un cargo o ejercer una función. El proceso de revisión de antecedentes también busca proveer un nivel de seguridad que indique que los antecedentes no levantan preocupaciones razonables sobre si dicha incorporación pudiera exponer al grupo a niveles inaceptables de riesgo.

Como pre-filtro para todos los postulantes, se realiza un test o lista de chequeo institucional. Las revisiones de antecedentes, según lo permitido por la ley, incluye cuando es posible:

- Certificado de estudios y verificación de estos especialmente para los trabajadores y contratistas del área clínica
- Currículum Vitae en formato de la función publica
- Referencias laborales a ex empleados
- Curso OS10 (Cargos de seguridad en sistemas de información)

De acuerdo a los procesos y procedimientos involucrados en la actualización de la pagina web y los sistemas de información, se hace necesario determinar las siguientes acciones:

a. Efectuar el back up del servidor cada semana
b. Efectuar los back up de informes institucionales e información de la entidad de los equipos de sistemas portátiles asignados cada 15 días y dejar esta información grabada en un disco externo bajo la responsabilidad de la oficina de sistemas de información y comunicaciones

9.5 Consciencia de Seguridad

La ESE cuenta con un programa de concientización continua de seguridad, el cual emplea diversos canales para realizar la bajada de información con el fin de involucrar al personal. Este programa cuenta principalmente con:

· Capacitaciones presenciales y/o virtuales;
· Publicación en intranet/carteles;
· Campañas de Awareness o conciencia de seguridad
· Cursos de inducción para nuevos colaboradores.

9.6 Política de seguridad de la ESE

La ESE ha desarrollado, para todo el equipo de trabajo, una política de Seguridad de la Información, en la que se establecen lineamientos para sus colaboradores y terceros involucrados. La política provee un marco de trabajo para todos los procesos y mecanismo de seguridad. Define los objetivos de seguridad, clasificación, responsabilidades y principios fundamentales para asegurarla de acuerdo con los objetivos del negocio. Las políticas de la ESE incluyen, pero no se limitan a:

- Responsabilidades definidas de seguridad de la información para colaboradores, contratistas y terceros
- Testeos para identificar controles faltantes o deficientes
- Política y lineamientos para todos los usuarios, acerca de uso aceptable de correo e internet
- Criterios definidos para el control de acceso, incluyendo la necesidad de conocer, principio de privilegio, usuario / ID único, complejidad de contraseñas, aprobaciones de acceso, transferencia de recertificación y procesos de abandono (desvinculación), acceso privilegiado y controles de acceso remoto

- Ciclos de vida de desarrollo de software para aplicaciones que incluyen revisión de código, separación de tareas, revisiones de seguridad para servicios web, entre otros.
- Control de cambios y respaldo de información para la continuidad del servicio asistencial.
- Procesos definidos para clasificación de información
- Instrucciones detalladas para encriptación, transferencia segura y destrucción de datos
- Políticas del entorno del usuario final, que abarcan la extracción de datos, el procesamiento de datos no gestionados por TI (informática del usuario final), clasificación de datos, etiquetado, destrucción segura del almacenamiento y trabajo remoto.
- Configuración técnica y configuración de control para infraestructura de TI, redes y plataformas.
- Seguridad física La política define requerimientos mínimos para:
  - La gestión y gerenciamiento de la información
  - El control de accesos
  - La seguridad física
  - Las comunicaciones, operaciones y desarrollo de sistemas

9.7 Gestión de Riesgos

La ESE utiliza la gestión de riesgos en todas sus líneas clave de defensa para identificar, informar y gestionar los riesgos en toda la empresa. Los marcos de seguridad de la información dentro de la ESE siguen estándares de mejores prácticas a nivel nacional ordenadas por el MINTIC. Las evaluaciones de riesgo se realizan periódicamente para abordar cambios en requisitos de seguridad de la información del grupo o el apetito de riesgo y cuando ocurren cambios significativos. La ESE realiza evaluaciones de riesgo en la variedad de activos estratégicos/críticos dentro de la empresa. Estos pueden ser activos físicos, personas, software

e información. Realizar, además, evaluaciones periódicas del riesgo de seguridad de la información sobre las tecnologías de aplicaciones e infraestructura para:

- Identificar, cuantificar y gestionar los riesgos de seguridad de la información para alcanzar los objetivos comerciales.
- Proporcionar medios para identificar actividades y factores que representan el mayor riesgo de seguridad para la ESE.
- Asegurar que los problemas de seguridad de la información se gestionen de acuerdo con su calificación de riesgo y que los controles sean proporcionales al nivel de riesgo descubierto.
- Proporcionar una visión empresarial de los riesgos de seguridad de la información y los planes de corrección respectivos para desarrollar la estrategia de seguridad de la información.
- Planificar el despliegue de recursos en áreas que brinden la mayor reducción de riesgos para la información del usuario / empresa.
- Evaluar todos los aspectos de los riesgos, amenazas y vulnerabilidades de seguridad de la información de nuestros activos y documentos.

9.8 Gestión de Accesos

Una la oficina de sistemas de información, posee y opera el control de gestión de acceso dentro de la ESE, esto garantiza una gestión de acceso alineada con el regulador y orientada por políticas en todo el ciclo de vida de los controles de soporte. Los servicios/responsabilidades del equipo de gestión de identidad y acceso incluyen:

- Controles de nuevos colaboradores, colaboradores que abandonan la empresa o se mueven internamente, incorporando segregación de funciones para garantizar que se gestionen y/o mantengan los derechos autorizados de nivel correspondiente de privilegios para todas las actividades de los usuarios

- Controles de gestión de acceso privilegiado con la debida justificación y autorización, incorporando la validación de actividades a través de un proceso de registro y monitoreo.
- Acceso a controles de recertificación para garantizar que las cuentas y derechos asociados sean revisados, mantenidos o revocados, periódicamente, por el revisor apropiado.

9.9 Seguridad de Redes

Para permitir una gestión eficaz, la ESE utiliza diversas tecnologías implementadas estratégicamente en toda su red, las cuales se describen a continuación:

- Gestión de redes inalámbricas
- Protección de denegación de Servicio
- Filtro de acceso a internet
- Testeo de Infraestructura de Seguridad
- Auditoría Externa de Cumplimiento y seguridad de la Información

10. LISTADO DE DOCUMENTOS CONFIDENCIALES

Para la Ese y de acuerdo con la normatividad institucional, se consideran CONFIDENCIALES los siguientes documentos:

a. HISTORIA CLINICA

ARTICULO 34, Ley 23 de 1981. La historia clínica es el registro obligatorio de las condiciones de salud del paciente. Es un documento privado sometido a reserva que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la Ley.

ARTICULO 1, Ley 1995 de 1999. DEFINICIONES. a) La Historia Clínica es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los

actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley.

ARTÍCULO 13.- CUSTODIA DE LA HISTORIA CLÍNICA. La custodia de la historia clínica estará a cargo del prestador de servicios de salud que la generó en el curso de la atención, cumpliendo los procedimientos de archivo señalados en la presente resolución, sin perjuicio de los señalados en otras normas legales vigentes. El prestador podrá entregar copia de la historia clínica al usuario o a su representante legal cuando este lo solicite, para los efectos previstos en las disposiciones legales vigentes.

PARÁGRAFO PRIMERO. Del traslado entre prestadores de servicios de salud de la historia clínica de un usuario, debe dejarse constancia en las actas de entrega o de devolución, suscritas por los funcionarios responsables de las entidades encargadas de su custodia.

PARÁGRAFO SEGUNDO. En los eventos en que existan múltiples historias clínicas, el prestador que requiera información contenida en ellas, podrá solicitar copia al prestador a cargo de las mismas, previa autorización del usuario o su representante legal.

PARÁGRAFO TERCERO. En caso de liquidación de una Institución Prestadora de Servicios de Salud, la historia clínica se deberá entregar al usuario o a su representante legal. Ante la imposibilidad de su entrega al usuario o a su representante legal, el liquidador de la empresa designará a cargo de quien estará la custodia de la historia clínica, hasta por el término de conservación previsto legalmente. Este hecho se comunicará por escrito a la Dirección Seccional, Distrital o Local de Salud competente, la cual deberá guardar archivo de estas comunicaciones a fin de informar al usuario o a la autoridad competente, bajo la custodia de quien se encuentra la historia clínica.

Adicionalmente es necesario observar el contenido de la Sentencia T-1051 de 2008, donde manifiesta que "la historia clínica y su contenido y los informes que de la misma se deriven, están sujetos a la reserva, y por lo tanto, solo pueden ser conocidos por el médico y su paciente."
En este sentido la entidad debe generar una circular que establezca los procesos y procedimientos de solicitud de la historia clínica.

b. Procesos a favor y en contra de la Entidad

Guardan la reserva relacionada con el proceso judicial, relación cliente/abogado, cliente/representando y la reserva como documento de interés solo para las partes involucradas.

CUMPLASE,

JARQUIN EBERTO MELENDEZ BARON
GERENTE ESE CAMU DEL PRADO DE CERETE

IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

	Nº	IDENTIFICACION DE RIESGOS	FECHA DE IDENTIFICACIO N DE RIESGO	ANALISIS DEL RIESGO			VALORACION INICIAL DEL RIESGO			TRATAMIENTO Y SEGUIMIENTO DEL RIESGO						
				CAUSAS	CONSECUENCIAS	BARRERAS DE SEGURIDAD EXISTENTES	VALOR DE PROBABILIDAD	VALOR DE IMPACTO	NIVEL DEL RIESGO	BARRERAS DE SEGURIDAD A IMPLEMENTAR	RESPONSABLE DEL SEGUIMIENTO	INDICADOR	LINEA BASE	META	RESULTADOS DE EFECTIVIDAD DE LAS	VALORACION DEL RIESGO DESPUES DE CONTROLES (Control Interno)
TEC	1	Fluido eléctrico, daño en hardware especializado como servidores, swicth principales	22-01-2021	- Daño en hardware y software especializado **redes**: daño en swicth **Servidores**: daño fisico y lógico de los principales servidores de producción del HCI - Caidas y variaciones en el fluido eléctrico	Posible daño en los equipos	- Los Swicth principales distribuidos por la ESE pueden ser configurados como de acceso, distribución ó núcleo en caso de daño se algún dispositivo, además se cuenta con planta de energía que reduce los daños por perdida de información y regula la atención al usuario en ventanillas de facturación. - Plan de contingencia en caso de caída del sistema de información principal - El servidor principal de la ESE el cual contiene el sistema de información SYSTEMFACT trabaja con un motor de bases de datos que permite hacer la replicación de seguridad y habilita la información de carácter permanente - Cronograma de mantenimiento preventivo y correctivo de computadores y equipo de redes de datos - Firewall configurado	2	2	4	- Implementación de estrategia MIPG en sus componentes: TIC para Gobierno Abierto TIC para Servicios TIC para la gestión Seguridad y privacidad de la información Habilitación del los indicadores ITA	Proceso de sistemas y comunicaciones, gestión de calidad, control interno,	Calificación de autodiagnóstico de componentes de MIPG superior al 60%	100%	100%	100%	

JARQUIN EBERTO MELENDEZ BARON
GERENTE ESE CAMU DEL PRADO DE CERETE