ESE Hospital Regional de Duitama

Plan de servicio: Plan De Seguridad Y Privacidad De La Información

ESE Hospital Regional de Duitama

Proceso: Gestión de la Información
Subproceso: Tecnologías de la información
Plan de servicio: Plan Estratégico De Tecnologías De La Información

Código	
Fecha	
Versión	

Estratégico	Misional	Apoyo	Evaluación

Objetivo

Establecer una estrategia de Seguridad de la Información que defina los lineamientos del Modelo de Seguridad y Privacidad de la Información y la Política de Seguridad y Privacidad de la Información, con el fin de garantizar la confidencialidad, integridad y disponibilidad de los activos de información.

OBJETIVOS ESPECÍFICOS

- Fomentar la adopción de mejores prácticas en seguridad de la información, sirviendo como base para la aplicación del concepto de Seguridad Digital.
- Actualizar el **Modelo de Seguridad y Privacidad de la Información (MPSI)**, con el propósito de fortalecer la protección de la información y los sistemas ante accesos, usos, divulgaciones, interrupciones o destrucciones no autorizadas.
- Garantizar un uso eficiente y seguro de los recursos de TI (humanos, físicos, financieros, tecnológicos, entre otros), asegurando la continuidad en la prestación de los servicios.
- Proteger los recursos de TI (humanos, físicos, financieros, tecnológicos, entre otros) para mantener la operación ininterrumpida de los servicios.
- Difundir e implementar la Estrategia de Seguridad de la Información en la organización.

Responsable

Líder Tecnología De La Información (Tecnologías de la Información)

Alcance

Establece los documentos institucionales y los lineamientos de la estrategia de Seguridad y Privacidad de la Información de la E.S.E. Hospital Regional de Duitama para el período 2024-2027. Estos lineamientos deberán ser conocidos y acatados por empleados, contratistas, terceros y demás partes interesadas que accedan, almacenen, procesen o transmitan información de la institución o de sus pacientes.

Introducción

El Plan de Seguridad y Privacidad de la Información define los lineamientos que viabilizan la gestión y administración de los planes y procedimientos de seguridad de la información, estableciendo las prácticas de protección aplicadas en la institución. Este plan se desarrolla en concordancia con el compromiso directivo asumido en la materia y en alineación con los lineamientos de la Política de Gobierno Digital dentro del Modelo Integrado de Planeación y Gestión (MIPG).

El presente plan orienta la gestión del área de tecnologías de la información durante el período 2024-2027, a través de una serie de acciones estratégicas que fortalecen la seguridad de la información en la E.S.E. Hospital Regional de Duitama. Cada año se priorizarán actividades específicas, con el objetivo de mejorar progresivamente la seguridad y privacidad de la información en la entidad.

Responsables

Tabla 1 . Responsables del Plan de Seguridad y Privacidad.

PROCESO O AREA	ROL O ACTIVIDADES
Tecnologías de la Información	Encargado de la gestión de la seguridad y privacidad digital sobre los activos de la información de la entidad.
Gestión Documental	Es el encargado de preservar la seguridad y confidencialidad de la información física.
Planeación	Encargado de la verificación en el cumplimiento de las actividades de seguridad y privacidad programadas.

Fuente/: Diseño de la E.S.E Hospital Regional de Duitama

Marco Legal y/o Teórico

Tabla 2. Marco Normativo para la realización del Plan de Seguridad y Privacidad de la Información.

DENOMINACIÓN	FECHA DE EMISIÓN	EMISOR	DESCRIPCIÓN GENERAL / APLICABILIDAD
ISO – IEC 27001:2013	2013	Congreso de la República	Sistema de Gestión de la Seguridad de la Información
Resolución No. 242	03/11/2020	E.S.E. Hospital Regional de Duitama	Política de Seguridad Privacidad de la Información y Seguridad Digital.
Guía v 3.0.2	29/07/2016	MINTIC	Modelo de Seguridad y Privacidad de la Información

Fuente/: Diseño de la E.S.E Hospital Regional de Duitama

Diagnostico y/o situación actual

ANALISIS DE LA SITUACIÓN ACTUAL

La E.S.E Hospital Regional de Duitama, durante la vigencia 2020 a 2024, a avanzado en la gestión de actividades de seguridad y privacidad de la información, siguendo la planeación del Plan de Seguridad y Privacidad de la Información, consiguiendo de esta forma:

- Actualizar el programa institucional, Modelo de Seguridad y Privacidad de la Información.
- Normalizar un plan anual de capacitaciones y sensibilización sobre seguridad de la información.
- Actualizar el Plan de Tratamiento de Riesgos de Seguridad de la Información.
- Normalizar el Plan de continuidad del negocio para los servicios tecnológicos y procesos críticos de la entidad.
- Integrar la seguridad de la información en los procesos institucionales.
- Definir procedimientos para la gestión de usuarios.

Que, teniendo en cuenta la planeación realizada en el año 2024, se tiene un progreso del 80%, finalizando la vigencia con la ejecución de 2 actividades principales, las cuales tienen un costo de inversión producto de toda la gestión realizada durante los tres años.

Tabla 3. Porcentaje de ejecución por actividad.

No.	% Ejecución de la actividad	Actividad
Iniciativa 1 Act. 1	100%	**Implementar, evaluar y mejorar el Plan de Seguridad y Privacidad de la Información**
Iniciativa 2 Act. 1	100%	**Integrar la seguridad de la información en los procesos institucionales**
Iniciativa 3 Act. 1	100%	**Diseñar y documentar programa anual de capacitaciones y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas**
Iniciativa Act. 2	100%	**Implementar y evaluar el programa anual de capacitación y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas**
Iniciativa 4 Act. 1	100%	**Actualizar la matriz de activos de información y publicaciones por criticidad para la entidad e identificar los riesgos de seguridad de la información asociados**

Iniciativa 5 Act. 1	100%	**Gestionar el Tratamiento de riesgos de seguridad de la información de los riesgos identificados en cada uno de los procesos.**
Iniciativa 6 Act. 1	100%	**Diseñar los planes de continuidad del negocio que contemplen los procesos críticos para la entidad**
Iniciativa 7 Act. 1	100%	**Documentar, Implementar y realizar pruebas de los planes de continuidad de negocio, así mismo Aprobar los planes de continuidad por la alta dirección.**
Iniciativa 7 Act. 1	30%	**Gestionar la adquisición de herramientas para soportar la Infraestructura del Datacenter, en esquemas de alta disponibilidad para dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core**
Iniciativa 7 Act. 10	100%	**Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la confidencialidad de la información.**
Iniciativa 10 Act. 1	100%	**Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.**
Iniciativa 11 Act. 1	100%	**Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.**
Iniciativa 12 Act. 1	50%	**Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web**
Iniciativa 13 Act. 1	50%	**Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo todos los procesos de la entidad.**
Iniciativa 14 Act. 1	50%	**Implementar y monitorear los indicadores del sistema de gestión de seguridad de la información**

Definiciones

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

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).

Activos de información: Los activos de información son el resultado de la construcción de un inventario y clasificación de los activos que posee la entidad de acuerdo con la Política General de Seguridad y Privacidad de la información, la cual determina que activos posee la entidad, cómo deben ser utilizados, así como los roles y responsabilidades que tienen los funcionarios sobre los mismos. 1 en cuanto a 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/IEC27000).

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. (ISO/IEC 27000).

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

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

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Control: Es toda actividad o procesos encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal 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.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

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).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida
personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Disponibilidad: Asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan.

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Evento de seguridad de la información: Es la presencia identificada de un estado que indica un incumplimiento posible de la política de seguridad de la información, una falla de los controles de seguridad, o una situación desconocida que puede ser pertinente para la seguridad de la información.
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).

Guía: Documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de

información.

Incidente de seguridad de la información: Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de los activos de información. Los incidentes de seguridad de la información son hechos inevitables sobre cualquier ambiente de información, y estos pueden ser bastante notorios e involucrar un impacto fuerte sobre la información de la organización.

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6) .

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712
de 2014. (Ley 1712 de 2014, art 6).

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

MSPI: Modelo de Seguridad y Privacidad de la Información

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

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).

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

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Propietario/responsable de activo de información: Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

Política: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.

Procedimiento: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas
apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

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).

Servicio: Es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o 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).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

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/IEC27000).

Usuario: Es el nombre (o alias) que se le asigna a cada persona para ser identificado por el servidor, de esta manera el proveedor de Internet o de correo electrónico lo identifica, es única en cada servidor, y cada usuario tiene asignado una contraseña para poder acceder a su cuenta.

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

Recursos, Materiales, Insumos y Equipos

La E.S.E Hospital Regional de Duitama a través de la Resolución No. 242 de 03 de noviembre de 2020 estableció la Política de Seguridad, Privacidad de la Información y Seguridad Digital, en la cual se ha se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes, en concordancia con la misión y visión de la entidad y los procesos establecidos para su operación con lo cual reconoce la información como un activo importante para la atención de los pacientes y el desarrollo de sus procesos internos, lo que requiere definir lineamientos que permitan mitigar los posibles riesgos para la Información.

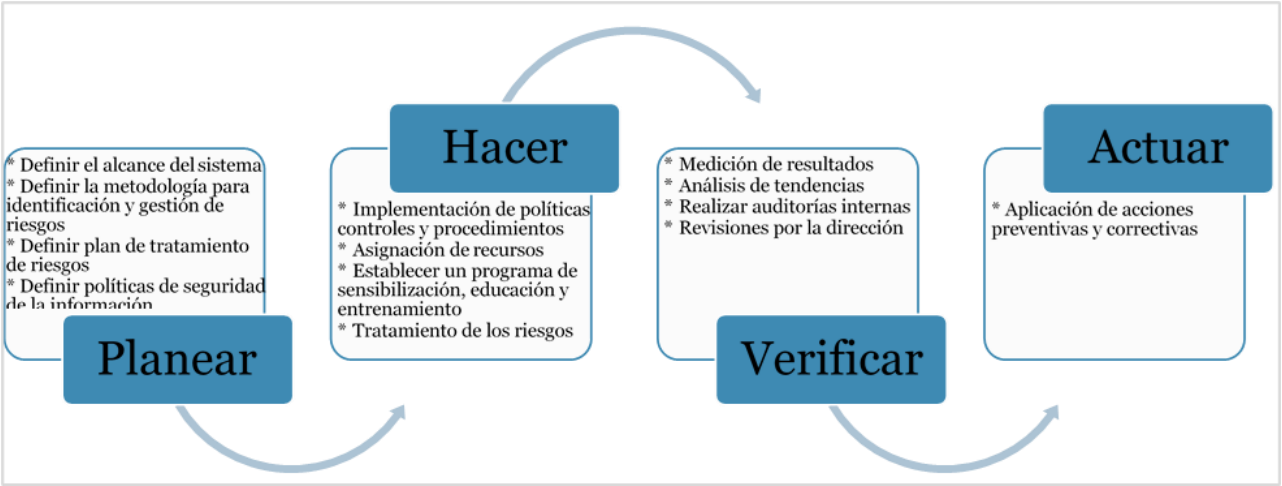
Desarrollo

LINEAMIENTOS CONEPTUALES Y METODOLOGICOS

La E.S.E. Hospital Regional de Duitama adopta mediante políticas, programas, lineamientos, procedimientos, estrategias y guías la adopción del proceso de seguridad y privacidad de la información.

El modelo del Sistema de Gestión de Seguridad de la Información (SGSI) de la E.S.E Hospital Regional de Duitama se encuentra basado en el ciclo de mejoramiento continuo PHVA (Planear, hacer, verificar y actuar), el cual asegura que el SGSI esté expuesto a revisiones continuas cuando existe un cambio importante en la infraestructura o se requiera mejorar su efectividad dependiendo de las mediciones de parámetros claves de su operación. Se cuenta, entonces, con un ciclo de mejoramiento continuo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.

Ilustración 1Ciclo PHVA adoptado por la institución



Fuente/: Ciclo PHVA de la E.S.E. Hospital Regional de Duitama

PROGRAMA: MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El objetivo del programa es definir un sistema de gestión de seguridad de la información y seguridad digital para la E.S.E Hospital Regional de Duitama, que contemple su operación en un ciclo PHVA (Planear, Hacer, Verificar y Actuar) mediante las fases de diagnóstico, planificación, operación, evaluación de desempeño y mejoramiento continuo.

POLÍTICA DE SEGURIDAD, PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL.

La entidad se compromete con la revisión y actualización de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes, en concordancia con la misión y la visión de la entidad y los procesos establecidos para su operación.

POLITICA DE GOBIERNO DIGITAL Y SEGURIDAD DIGITAL

La E.S.E Hospital Regional de Duitama, se compromete a definir y aplicar estrategias de transformación digital y aprovechamiento de las TIC, para fortalecer la relación con el usuario, mejorando la prestación de servicios de salud, generando confianza institucional, a partir de infraestructura tecnológica, seguridad y privacidad de la información, cultura y apropiación, servicios ciudadanos digitales, decisiones basadas en datos, estado abierto, proyectos innovadores y soluciones novedosas.

POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES.

La E.S.E Hospital Regional de Duitama se compromete a informar de manera suficiente a todos sus grupos de interés, sobre el derecho constitucional que tienen todas las personas en su calidad de titulares de la información a conocer, actualizar, rectificar o suprimir las información y datos personales que se hayan recogido sobre ellas en bases de datos o archivos de la entidad. En su condición de responsable y/o encargada del tratamiento de la información, actuará con responsabilidad al momento de recopilar información durante el desarrollo de sus procesos enmarcados en el cumplimiento de la misión institucional y le dará exclusivamente el uso y tratamiento permitido por la ley. La presente política de tratamiento de datos personales, se basa en los consagrado en la Ley 1581 de 2012, el Decreto Reglamentario 1377 de 2013, en concordancia con la Constitución Política de Colombia y demás disposiciones aplicables a la materia, junto con sus modificaciones, supresiones, ampliaciones y correcciones.

COMPROMISO DE LA DIRECCIÓN

La Junta Directiva y Alta Dirección de la E.S.E Hospital Regional de Duitama muestra su compromiso y apoyo en el diseño, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información a través de la asignación de recursos, los lineamientos de seguridad y el establecimiento del Gobierno de seguridad, cuya conformación y responsabilidades se describen a

continuación.

Por situación actual se entiende el nivel de madurez que posee en este momento La E.S.E Hospital Regional de Duitama con relación a la seguridad de la información. El proceso por el cual se lleva a cabo esta estimación del nivel de madurez se denomina Instrumento de diagnóstico del Modelo de Seguridad y Privacidad de la Información MSPI de MINTIC.

COMITÉ DE SEGURIDAD

Los temas de seguridad y Privacidad de la información al interior de la ESE HRD, son incorporados dentro de la temática a tratar en el comité institucional de gestión y desempeño.

ANÁLISIS Y PRIORIZACIÓN DE INICIATIVAS

La E.S.E Hospital Regional de Duitama ha identificado las siguientes iniciativas buscando garantizar el avance de la institución en la construcción de una arquitectura de seguridad de la información.

Tabla 4. Análisis y Priorización de iniciativas TI.

No.	Descripción	Modelo de seguridad de la información	Gestión de riesgos de seguridad	Desarrollo del programa de seguridad de la Información	Gestión de incidentes de seguridad de la información
1	Documentar, Implementar, evaluar y mejorar el Plan de Seguridad y Privacidad de la información	X			
2	Definir e integrar la seguridad de la información en los procesos institucionales buscando asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proceso	X			
3	Diseñar, documentar, implementar, evaluar y mejorar un programa anual de capacitaciones y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas	X			
4	Actualizar Plan de Tratamiento de Riesgos de seguridad de la información.		X		
5	Actualizar los activos de información y realizar su valoración o diagnostico por criticidad para la entidad e identificar los riesgos de seguridad de la información asociados		X		
6	Diseñar los planes de continuidad del negocio que contemplen los procesos críticos para la entidad		X		
7	Documentar, Implementar y realizar pruebas de los planes de continuidad de negocio, así mismo Aprobar los planes de continuidad por la alta dirección.		X		
8	Implementar arquitecturas redundantes en dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core			X	
9	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la confidencialidad de la información.			X	
10	Monitorear el cumplimiento del ciclo de vida de gestión de usuarios (creación, modificación, activación, desactivación, eliminación, entre otros) verificando que se cumple para todas las aplicaciones.			X	

11	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web			X	
12	Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo todos los procesos de la entidad.			X	
13	Implementar y monitorear los indicadores del sistema de gestión de seguridad de la información	X			

Fuente/: Elaboración propia de la Institución.

DEFINICIÓN DEL PORTAFOLIO DE PROYECTOS

En esta etapa, después del análisis y priorización de iniciativas, se define el portafolio de proyectos del plan de seguridad y privacidad de la información, agrupados en proyectos relacionados con:

1. Gobierno o modelo de seguridad de información.
2. Gestión de riesgos de Seguridad.
3. Desarrollo y gestión del plan de seguridad de la información.
4. Gestión de incidentes de seguridad de la información.

Tabla 5. Definición del portafolio de proyectos TI.

	Iniciativa	**Proyectos**		
		Descripción	**Avances**	**Requiere recursos financieros**
1	Documentar, Implementar, evaluar y mejorar el Plan de seguridad y Privacidad de la información.	Implementar, evaluar y mejorar el Plan de Seguridad y Privacidad de la Información	Ejecutado	SI
2	Definir e integrar la seguridad de la información en los procesos institucionales buscando asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proceso	Integrar la seguridad de la información en los procesos institucionales	Ejecutado	NO
3	Diseñar, documentar, implementar, evaluar y mejorar un programa anual de capacitaciones y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas	Diseñar y documentar programa anual de capacitaciones y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas	Ejecutado	NO
		Implementar y evaluar el programa anual de capacitación y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas	Ejecutado	NO
4	Actualizar los activos de información y realizar su valoración por criticidad para la entidad e identificar los riesgos de seguridad de la información asociados	Actualizar la matriz de activos de información y publicaciones por criticidad para la entidad e identificar los riesgos de seguridad de la información asociados	Ejecutado	NO
5	Gestionar el Tratamiento de riesgos de seguridad de la información de los riesgos identificados en cada uno de los procesos.	Gestionar el Tratamiento de riesgos de seguridad de la información de los riesgos identificados en cada uno de los procesos.	Ejecutado	NO
6	Diseñar los planes de continuidad del negocio que contemplen los procesos críticos para la entidad	Diseñar los planes de continuidad del negocio que contemplen los procesos críticos para la entidad	Ejecutado	NO

7	Documentar, Implementar y realizar pruebas de los planes de continuidad de negocio, así mismo Aprobar los planes de continuidad por la alta dirección.	Documentar, Implementar y realizar pruebas de los planes de continuidad de negocio, así mismo Aprobar los planes de continuidad por la alta dirección.	Ejecutado	NO
8	Implementar arquitecturas redundantes en dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core	Gestionar la adquisición de herramientas para soportar la Infraestructura del Datacenter, en esquemas de alta disponibilidad para dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core.	En Ejecución	SI
9	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la confidencialidad de la información.	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la confidencialidad de la información.	Ejecutado	NO
10	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.	Ejecutado	NO
11	Monitorear el cumplimiento del ciclo de vida de gestión de usuarios (creación, modificación, activación, desactivación, eliminación, entre otros) verificando que se cumple para todas las aplicaciones.	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.	Ejecutado	NO
12	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web	En Ejecución	SI
13	Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo todos los procesos de la entidad.	Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo todos los procesos de la entidad.	Ejecutado	SI
14	Implementar y monitorear los indicadores del sistema de gestión de seguridad de la información	Implementar y monitorear los indicadores del sistema de gestión de seguridad de la información	En Ejecución	NO

Fuente/: Elaboración propia de la Institución.

PLAN DE ACCIÓN

PRIORIZACIÓN DE LOS PROYECTOS a 2024

Tabla 6. Priorización de proyectos de seguridad TI.

	Priorización de los Proyectos				
	Descripción	Prioridad Año 2021	Prioridad Año 2022	Prioridad Año 2023	Prioridad Año 2024
1	Implementar, evaluar y mejorar el Plan de Seguridad y Privacidad de la Información	X			
2	Integrar la seguridad de la información en los procesos institucionales	X			
3	Diseñar y documentar programa anual de capacitaciones y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas		X		
	Implementar y evaluar el programa anual de capacitación y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas		X		
4	Actualizar la matriz de activos de información y publicaciones por criticidad para la entidad e identificar los riesgos de seguridad de la información asociados	X			
5	Documentar y normalizar el Plan de Tratamiento de riesgos de Seguridad de la información.		X		
6	Diseñar los planes de continuidad del negocio que contemplen los procesos críticos para la entidad			X	
7	Documentar, Implementar y realizar pruebas de los planes de continuidad de negocio, así mismo Aprobar los planes de continuidad por la alta dirección.			X	

8	Gestionar la adquisición de herramientas para soportar la infraestructura del Datacenter, en esquemas de alta disponibilidad para dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core.		X
10	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.	X	
11	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.	X	
12	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web		X
14	Implementar y monitorear los indicadores del sistema de gestión de seguridad de la información		X

Fuente/: Elaboración propia de la Institución.

El plan estratégico corresponde a la ejecución de los proyectos definidos en el portafolio de proyectos de seguridad de la información que aportan al cumplimiento de los objetivos de seguridad de la información y al Plan Estratégico de las Tecnologías de la Información y Comunicaciones PETI.

PLAN DE ACCIÓN VIGENCIA 2025

Tabla 6. Plan de Acción para la vigencia 2025.

COMPONENTE	NO.	ACTIVIDAD	RESULTADO / SOPORTE	RESPONSABLE	FECHA
Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	1	Implementar una solución profesional de seguridad perimetral, basada por el cuadrante magico de Gartner, cuya administración sea realizada por una empresa con experiencia en ciberseguridad y se garantice la gestión de politicas de seguridad y correcto funcionamiento de los equipos entregados.	Informe de implementación de una solución de seguridad perimetral y conexión entre sedes anexas.	Líder de Tecnologías de la Información.	30/06/2025
	2	Monitorear los indicadores del sistema de gestión de seguridad de la información	Realizar seguimiento a los indicadores	Líder de Tecnologías de la Información.	30/06/2025

Bibliografía

MINISTERIO DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (Febrero de 2021). Modelo de Seguridad y Privacidad de la Información Anexo 1.

Términos y Definiciones

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

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).

Activos de información: Los activos de información son el resultado de la construcción de un inventario y clasificación de los activos que posee la entidad de acuerdo con la Política General de Seguridad y Privacidad de la información, la cual determina que activos posee la entidad, cómo deben ser utilizados, así como los roles y responsabilidades que tienen los funcionarios sobre los mismos. 1 en cuanto a 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. (ISO/IEC 27000).

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias objetivas y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría (2018, GTC 19011)

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Control: Es un mecanismo preventivo y correctivo adoptado por la administración de una dependencia o entidad que permite la oportuna detección y corrección de desviaciones, ineficiencias o incongruencias en el curso de la formulación, instrumentación, ejecución y evaluación de las acciones, con el propósito de procurar el cumplimiento de la normatividad que las rige y las estrategias, políticas, objetivos, metas y asignación de recursos.

Datos Abiertos: son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

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).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Disponibilidad: Asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan.

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Evento de seguridad de la información: Es la presencia identificada de un estado que indica un incumplimiento posible de la política de seguridad de la información, una falla de los controles de seguridad, o una situación desconocida que puede ser pertinente para la seguridad de la información

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).

Guía: Documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.

Incidente de seguridad de la información: Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de los activos de información. Los incidentes de seguridad de la información son hechos inevitables sobre cualquier ambiente de información, y estos pueden ser bastante notorios e involucrar un impacto fuerte sobre la información de la organización.

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

MSPI: Modelo de Seguridad y Privacidad de la Información

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

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

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).

Política: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Procedimiento: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

Propietario/responsable de activo de información: Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo: Es la probabilidad que un incidente o evento adverso ocurra.

Seguridad de la Información: es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

Servicio: Es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o 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).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad: Capacidad para seguir la historia, la aplicación o localización de todo aquello que está en consideración en un medicamento, especialmente lo relacionado con el origen de los materiales, el proceso de elaboración y la localización del producto después de salir del sitio de elaboración.

Usuario: Es el nombre (o alias) que se le asigna a cada persona para ser identificado por el servidor, de esta manera el proveedor de Internet o de correo electrónico lo identifica, es única en cada servidor, y cada usuario tiene asignado una contraseña para poder acceder a su cuenta.

VULNERABILIDAD: Susceptibilidad o fragilidad física, económica, social, ambiental o institucional que tiene una comunidad de ser afectada o de sufrir efectos adversos en caso de que un evento físico peligroso se presente. Corresponde a la predisposición a sufrir pérdidas o daños de los seres humanos y sus medios de subsistencia, así como de sus sistemas físicos, sociales, económicos y de apoyo que pueden ser afectados por eventos físicos peligrosos.