PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 2024

INTRODUCCIÓN

La información que forma parte de una Entidad Pública es fundamental para su adecuado funcionamiento en el marco de la política pública y su conexión con los ciudadanos. No importa la naturaleza específica de la información manejada por la entidad; esta juega un papel esencial en el logro de sus objetivos. Por esta razón, proteger toda la información contra cualquier amenaza potencial, como alteraciones, mal uso o pérdida, entre otros eventos, se convierte en una medida crucial. Este resguardo no solo actúa como una salvaguarda, sino que también respalda el desarrollo normal de las actividades de la entidad o del Estado en su conjunto. La preservación de la integridad y confidencialidad de la información es esencial para mantener la eficiencia y transparencia en las operaciones gubernamentales y fortalecer la confianza de los ciudadanos en el proceso.

En el Marco de Seguridad del Modelo de Seguridad y Privacidad de la Información (MSPI), un aspecto fundamental es la Gestión de Riesgos, la cual desempeña un papel crucial en la toma de decisiones. En este contexto, dado que las entidades del Estado son el enfoque principal de esta guía y del MSPI en sí, se adopta la metodología de la "Guía de Riesgos" proporcionada por el Departamento Administrativo de la Función Pública (DAFP). La intención es integrar esta guía con lo que se ha implementado previamente dentro de la entidad en términos de otros modelos de gestión, aprovechando así el trabajo previo realizado en la identificación de riesgos para complementarlos con los riesgos específicos de seguridad de la información.

OBJETIVO

Organizar las estrategias a implementar para reconocer, evaluar, supervisar, comunicar y reducir los riesgos relacionados con la seguridad y la privacidad de la información.

OBJETIVOS ESPECÍFICOS

1. Designar claramente las tareas y responsabilidades a los miembros del personal que han sido identificados y recibido la formación necesaria en los procedimientos específicos del plan de contingencia. El propósito principal es asegurar que las personas asignadas estén adecuadamente preparadas para llevar a cabo las acciones requeridas en caso de una interrupción en las operaciones informáticas. Esto garantiza que, en situaciones de emergencia, se pueda contar con un equipo capacitado que actúe de manera eficiente y permita la restauración de las operaciones informáticas dentro del plazo establecido.
2. Establecer procesos y procedimientos bien definidos para abordar cualquier evento de seguridad que pueda impactar la disponibilidad de los recursos informáticos críticos. La idea central es asegurar que existan instrucciones claras y eficaces para manejar situaciones de seguridad, con el fin de garantizar la continuidad de los servicios informáticos esenciales. En otras palabras, se pretende contar con un conjunto de acciones y protocolos precisos que permitan responder de manera efectiva

ante eventos de seguridad, asegurando que los servicios informáticos fundamentales no se vean comprometidos.

3. Llevar a cabo ejercicios prácticos simulados de restauración con el propósito de asegurar el éxito de los procesos y procedimientos establecidos en el plan de contingencia. La finalidad es aumentar la confiabilidad y disponibilidad de los sistemas y servicios informáticos en la E.S.E. Universitaria del Atlántico, mediante la realización de simulacros, se busca comprobar la eficacia del plan de contingencia, identificar posibles áreas de mejora y fortalecer la capacidad del personal para responder efectivamente en situaciones reales de interrupción informática, contribuyendo así a una mayor confiabilidad y disponibilidad de los sistemas y servicios esenciales.

ALCANCE

Este documento comenzará con el proceso de identificación de los riesgos de información asociados a las operaciones y servicios de la E.S.E. UNA. A lo largo de su desarrollo, se abordará de manera integral la evaluación y clasificación de estos riesgos. Finalmente, culminará con la implementación del plan diseñado específicamente para mitigar y gestionar eficazmente dichos riesgos.

APLICABLE A

Este documento tiene una aplicabilidad integral que abarca todos los ámbitos de operación de la E.S.E. Universitaria del Atlántico. Su alcance incluye no solo los procesos estratégicos y misionales, que son fundamentales para la consecución de los objetivos institucionales, sino también los procesos de apoyo que sustentan eficientemente las actividades clave. Además, se extiende a los procesos de evaluación, garantizando que las prácticas de identificación y tratamiento de riesgos se integren de manera coherente en todos los niveles y funciones de la E.S.E.

El proceso de gestión del riesgo, conforme a la Guía de Gestión del Riesgo del DAFP, se estructura en tres etapas fundamentales, sobre las cuales se apoyan las actividades destinadas a lograr una administración de riesgos alineada con las necesidades de la entidad. La primera y crucial etapa para avanzar de manera efectiva en todo el proceso es el "Compromiso de la alta y media dirección". Este compromiso, destacado en la guía, se erige como un factor primordial, ya que el auténtico respaldo de los directivos asegura en gran medida el éxito de cualquier iniciativa. La aprobación y participación activa de la dirección son esenciales en las decisiones, como se subraya tanto en la guía mencionada como en el Marco de Seguridad del Modelo de Seguridad y Privacidad de la Información (MSPI). La necesidad de contar con la aprobación de la dirección en cada fase del proceso se presenta como un requisito ineludible, consolidando así una gestión del riesgo eficaz.

El proceso de gestión integral del riesgo, en concordancia con la guía, requiere la designación de un directivo de primer nivel, preferiblemente el mismo encargado del desarrollo o mantenimiento del MECI y el Sistema de Gestión de la Calidad. Esta designación es esencial para asesorar y respaldar el proceso de diseño e implementación del Componente en cuestión, siguiendo la premisa de lograr una gestión integral del riesgo según lo establece el MSPI.

En segunda instancia, se destaca la importancia de la "Conformación de un Equipo MECI o de un grupo interdisciplinario". La idea de abordar integralmente los riesgos implica la necesidad de contar con un equipo que represente diversas áreas de la entidad. Esta diversidad permite obtener una visión completa de la entidad al analizar un mismo proceso. Es crucial incorporar los riesgos de seguridad durante el análisis del MECI o del modelo de Gestión de Calidad, alineando así los objetivos del MSPI.

Finalmente, se subraya la relevancia de la "Capacitación en la metodología". Aunque la capacitación es necesaria para que el equipo interdisciplinario pueda analizar los riesgos de seguridad, es vital que este equipo esté integrado por miembros del proyecto MSPI. Esto garantiza un conocimiento profundo del contexto organizacional en todos los aspectos del desarrollo del MSPI, permitiendo una implementación efectiva y coherente con los objetivos establecidos.

MARCO NORMATIVO

- Decreto 1360 de 1989 Presidencia de Colombia Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.
- Decreto 2150 de 1995 MINISTERIO DE JUSTICIA Y DEL DERECHO Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.
- Ley 572 de 1999 Congreso de la República Comercio Electrónico, Firmas Digitales, Intercambio electrónico de datos.
- Documento Conpes 3072 de 2000 Conpes Agenda de Conectividad.
- Decreto 3816 de 2003 Presidencia de Colombia Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública.
- Conpes 3292 de 2004 Conpes Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos.
- Ley 1273 de 2009 Congreso de la República Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1341 de 2009 Congreso de la República Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- Decreto 235 de 2010 Ministerio del Interior y Justicia Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.

- Conpes 3701 de 2011 Conpes Lineamientos de política para la Ciberseguridad y Ciberdefensa Ley 1581 de 2012 Congreso de la República Por el cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 884 de 2012 Presidencia de Colombia Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones
- Decreto 2364 de 2012 Ministerio del Interior y Justicia Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- Decreto 19 de 2012 Presidencia de Colombia Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- Ley 1712 de 2014 Congreso de la República Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1753 de 2015 Congreso de la República Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAÍS" "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 103 de 2015 Presidencia de Colombia Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1081 de 2015 Presidencia de Colombia Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República
- Decreto 1078 de 2015 Presidencia de Colombia Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 415 de 2016 Departamento Administrativo de la Función Pública Se modifica el decreto 1083 de 2015 y se definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública.
- Decreto 728 de 2017 Ministerio de las Tecnologías de la Información y las Comunicaciones Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto. Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de las zonas de acceso público a internet inalámbrico.
- Decreto 1413 de 2017 Ministerio de las Tecnologías de la Información y las Comunicaciones En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales.
- Resolución 2710 de 2017 Ministerio de las Tecnologías de la Información y las Comunicaciones Por la cual se establecen lineamientos para la adopción del protocolo IPv6.
- Decreto 728 de 2017 Ministerio de las Tecnologías de la Información y las Comunicaciones Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto. Único Reglamentario del sector TIC.
- Decreto 1078 de 2015, para fortalecer el modelo de Gobierno.
- Circular 30 de 2017 Alta Consejería de TICs Implementación CSIRT de Gobierno Circular 36 de 2017 Alta Consejería de TICs Lineamientos de avance del modelo de seguridad y privacidad de

la información Resolución 3436 de 2018 Ministerio de las Tecnologías de la Información y las Comunicaciones Por la cual se reglamentan los requisitos técnicos, operativos y de seguridad que deberán cumplir las zonas de acceso a Internet inalámbrico de que trata el Capítulo 2, Título 9, Parte 2, Libro 2 del Decreto 1078 de 2015. Decreto 612 de 2018 Departamento Administrativo de la Función Pública Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- Decreto 1008 de 2018 Ministerio de las Tecnologías de la Información y las Comunicaciones Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones Circular 2 de 2018 Ministerio de las Tecnologías de la Información y las Comunicaciones Cumplimiento legal y normativo respecto a seguridad de la información.
- Conpes 3920 de 2018 Conpes Big Data, la política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales. Guía 6 de 2019 Ministerio de las Tecnologías de la Información y las Comunicaciones Guía para la construcción del Plan Estratégico de Tecnologías de Información PETI Ley 1955 del 2019 Presidencia de Colombia Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- Decreto 2106 de 2019 Departamento Administrativo De La Función Pública Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Pública Efectiva.
- Conpes 3975 de 2019 Conpes Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.
- Decreto 620 Departamento Estableciendo los lineamientos generales en el uso y operación de los Tipo de norma Entidad que expide Descripción normativa de 2020 Administrativo De La Función Pública servicios ciudadanos digitales Resolución 00500 de 2021 Ministerio de las Tecnologías de la Información y las Comunicaciones “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.
- Resolución 00500 de 2021 Anexo 1 Ministerio de las Tecnologías de la Información y las Comunicaciones Documento Maestro del Modelo de Seguridad y Privacidad de la Información Dirigida a las Entidades del Estado Directiva 09 de 2021 Secretaría Jurídica Distrital Buenas prácticas en el uso de fotografías y videos para la protección de derechos de autor.
  Decreto 612 de 2018: Por el cual se fijan las directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del estado.

MARCO CONCEPTUAL

GLOSARIO

- 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 el contexto de la seguridad de la información, se hace referencia a cualquier dato o componente vinculado con su manejo (sistemas, dispositivos de almacenamiento, instalaciones, personal, entre otros) que posea importancia para la organización, según la norma ISO/IEC 27000. En términos más específicos, un Activo de Información se define en el ámbito de la seguridad de la información como cualquier dato o componente que tiene valor para los procesos de la organización.
- Amenazas: Se refiere a una circunstancia que podría desencadenar un evento no deseado y, como consecuencia, ocasionar perjuicios a un sistema o a la organización. Esta definición se encuentra en concordancia con la norma ISO/IEC 27000.
- Administración del riesgo: Se refiere a un conjunto de mecanismos de control que, al interactuar entre sí, proporcionan a la entidad la capacidad para tomar las medidas necesarias. Esto permite gestionar eventos que podrían tener impactos negativos en el logro de los objetivos institucionales y proteger a la entidad de los efectos derivados de su ocurrencia.
- Análisis de brechas: es una herramienta que se utiliza para examinar y comparar la situación y el rendimiento real de una organización, estado o situación en un momento específico. Por otro lado, el análisis de riesgos es un método sistemático que implica la recopilación, evaluación, registro y difusión de información necesaria para hacer recomendaciones. Estas recomendaciones están orientadas a la adopción de una posición estratégica o la implementación de medidas específicas en respuesta a un peligro identificado.
- Auditoría: Procedimiento planificado y organizado de manera sistemática, independiente y debidamente registrado. Su propósito es obtener pruebas de auditoría con el fin de evaluar hasta qué punto se cumplen los criterios de auditoría establecidos. Este enfoque sigue las pautas de la norma ISO/IEC 27000.
- Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros. Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- Consecuencia: Resultado de un evento que afecta los objetivos.
- 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.
- Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.
- 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).

- Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).
- Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
- Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.
- Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.
- 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).
- Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo. Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados. Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000).
- Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
- Información: Conjunto de datos que tienen un significado.
- Integridad: Propiedad de la información relativa a su exactitud y completitud.
- Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.
- Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.
- Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.
- Parte interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- Probabilidad: Posibilidad de que una amenaza se materialice.

- 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).
- 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(Gobierno en Línea - Decreto 1151 de 2008) la correlativa obligación.
- Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.
- Procedimiento: Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.
- Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
- Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular.
- 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).
- Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
- Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.
- Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
- Riesgo de seguridad de la información: se refiere a la posibilidad de que una amenaza específica pueda explotar una vulnerabilidad, resultando en la pérdida o daño de un activo de información. Estos daños se manifiestan en la afectación de la confidencialidad, integridad o disponibilidad de la información. Es esencial reconocer que, en algunos casos, una amenaza puede transformarse en una oportunidad, generando beneficios para la organización. Por lo tanto, la gestión efectiva de este riesgo implica no solo mitigar las amenazas, sino también evaluar y aprovechar las oportunidades que puedan surgir, considerando siempre el equilibrio entre la seguridad de la información y el logro de los objetivos organizativos.
- Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.
- Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que

prestan al ciudadano. Preservación de la confidencialidad, integridad y disponibilidad de la información. Tolerancia al riesgo: son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable

- 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.
- 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).
- Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).
- Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos. Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

CONDICIONES GENERALES

Este plan de tratamiento de riesgos se propone realizar un análisis exhaustivo de los riesgos, abarcando desde la documentación hasta el diseño de recomendaciones, procedimientos y controles de seguridad en el ámbito del acceso a la información, tanto interna como externa. Es crucial destacar que no se establece un límite máximo o mínimo en la identificación de riesgos; la E.S.E. Universitaria del Atlántico se compromete a identificar cualquier riesgo que pueda afectar el logro de los objetivos de los procesos, sistemas de gestión, estándares, grupos de estándares y/o ejes trazadores de acreditación trazados. La identificación se llevará a cabo de manera objetiva para garantizar una evaluación precisa. La toma de decisiones estratégicas será fundamental en la gestión efectiva de riesgos, considerando opciones como la aceptación del riesgo con acciones para reducir su probabilidad o impacto, la transferencia a terceros, la eliminación mediante la interrupción de actividades causantes del riesgo, y la implementación de controles para mitigar riesgos identificados. Además, la E.S.E. UNA implementará procesos de formación y capacitación para desarrollar competencias en gestión del riesgo, fortaleciendo así la capacidad del personal para afrontar y mitigar eficazmente los riesgos. Este enfoque integral garantiza una gestión proactiva y efectiva de los riesgos en el entorno de la E.S.E. Universitaria del Atlántico.

ESTABLECIMIENTO DEL CONTEXTO:

En este paso, se busca comprender el entorno en el que opera la organización, identificando factores internos y externos que podrían afectar la seguridad de la información. Esto implica definir los objetivos, el alcance y los criterios de evaluación para la gestión del riesgo.

- VALORACIÓN DEL RIESGO:

La valoración del riesgo implica la identificación y análisis de los riesgos potenciales que podrían afectar la seguridad de la información. Se evalúan tanto la probabilidad de ocurrencia como el impacto en caso de que ocurran. Este proceso permite priorizar los riesgos y determinar cuáles requieren una atención inmediata.

- TRATAMIENTO DEL RIESGO:

Una vez identificados y evaluados los riesgos, se implementan estrategias para manejarlos. Esto incluye decidir cómo mitigar, transferir, aceptar o evitar los riesgos. Se desarrollan e implementan medidas de control y se establece un plan para gestionar los riesgos de manera efectiva.

- ACEPTACIÓN DEL RIESGO:

En algunos casos, la organización puede decidir aceptar ciertos riesgos cuando los costos asociados con la mitigación son desproporcionados en comparación con el beneficio esperado. Sin embargo, esta aceptación debe ser informada y documentada adecuadamente.

- COMUNICACIÓN DEL RIESGO:

La comunicación efectiva es esencial en la gestión del riesgo. Se deben establecer canales de comunicación claros para informar a todas las partes interesadas sobre los riesgos identificados, las estrategias de tratamiento y los resultados de la gestión del riesgo.

- MONITOREO Y REVISIÓN DEL RIESGO:

Este paso implica el seguimiento continuo de los riesgos identificados y las medidas de control implementadas. Se revisa periódicamente el contexto, se actualiza la valoración del riesgo y se ajustan las estrategias de tratamiento según sea necesario. La gestión del riesgo es un proceso iterativo y dinámico.

- CICLO DE MEJORA CONTINUA:

Implementación de un ciclo de mejora continua para perfeccionar el modelo de gestión de riesgos en seguridad de la información. Se aprovechan los resultados del monitoreo y las revisiones para ajustar y mejorar continuamente el enfoque de gestión de riesgos.

ESTABLECER EL CONTEXTO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Implica obtener una comprensión integral de los riesgos que podrían afectar el logro de los objetivos en estas áreas específicas. Este proceso implica una evaluación detallada de:

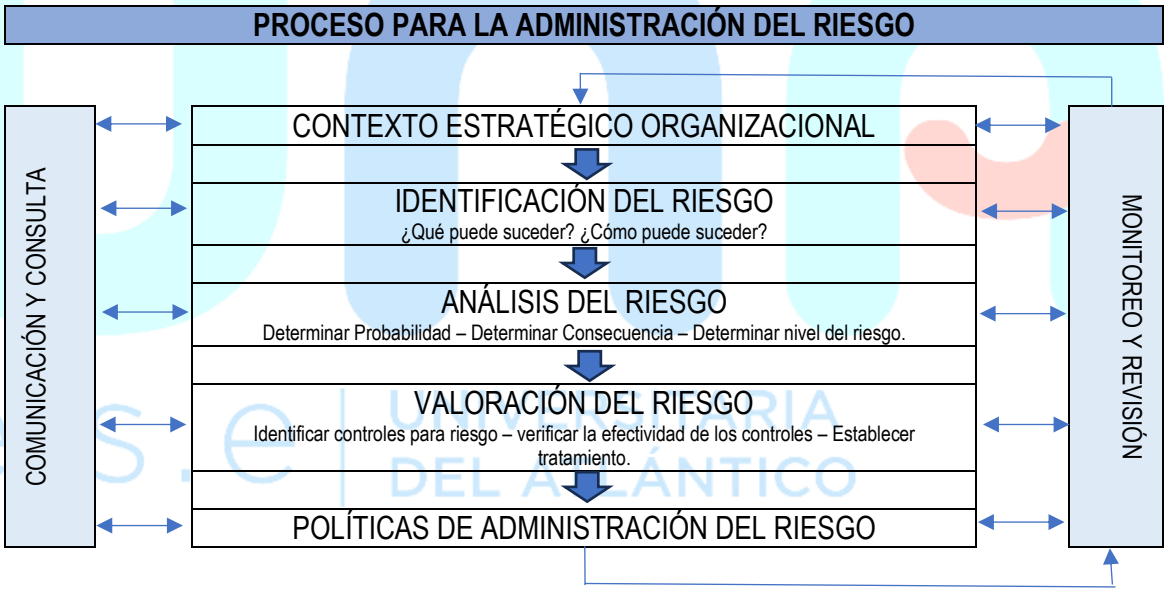
La estructura organizacional.

El modelo de operación por procesos

El cumplimiento de planes y programas

Los recursos físicos y tecnológicos disponibles

Para llevar a cabo este análisis, es esencial definir criterios específicos que permitan evaluar y cuantificar los riesgos asociados a la seguridad y privacidad de la información. Estos criterios actúan como marco de referencia para identificar, medir y gestionar los riesgos de manera efectiva en consonancia con los objetivos organizacionales y los estándares de seguridad y privacidad.



LOS CRITERIOS DE EVALUACIÓN DEL RIESGO

Los criterios de evaluación del riesgo en seguridad de la información constituyen un enfoque integral para determinar los riesgos a los que se enfrenta la E.S.E. Universitaria del Atlántico. Se consideran diversos aspectos clave:

- Valor Estratégico del Proceso de Información: Este criterio implica analizar la importancia estratégica del proceso de información en el contexto general de la E.S.E.UNA. Se evalúa cómo la seguridad de la información impacta directamente en los objetivos y metas estratégicas de la organización.
- Criticidad de los Activos de Información: La criticidad de los activos de información involucrados en el proceso es un factor crucial. Se examina la importancia de los datos y recursos específicos que son esenciales para el funcionamiento y la continuidad de las operaciones de la organización.

- Requisitos Legales y Reglamentarios, así como Obligaciones Contractuales: Este criterio aborda el cumplimiento de los requisitos legales y reglamentarios aplicables, así como las obligaciones contractuales relacionadas con la seguridad de la información. Se busca garantizar que la E.S.E. UNA cumpla con las normativas y acuerdos contractuales establecidos.
- Importancia de la Disponibilidad, Confidencialidad e Integridad de la Información: La evaluación de la importancia de la disponibilidad, confidencialidad e integridad de la información destaca la relevancia de preservar estos principios fundamentales de la seguridad de la información para asegurar el buen funcionamiento de las operaciones y la integridad de la E.S.E. UNA.
- Expectativas y Percepciones de las Partes Interesadas: Se considera la perspectiva de las partes interesadas, evaluando sus expectativas y percepciones en relación con la seguridad de la información. Esto asegura que se tenga en cuenta la satisfacción y confianza de los involucrados en la toma de decisiones.
- Consecuencias Negativas para el Buen Nombre y la Reputación de la E.S.E. UNA: Este criterio destaca la importancia de proteger la reputación y el buen nombre de la E.S.E. UNA. Se evalúan las posibles consecuencias negativas que podrían surgir en caso de incidentes de seguridad que afecten la percepción pública.

La inclusión de estos criterios en la evaluación del riesgo brinda una perspectiva completa, permitiendo a la E.S.E. UNA tomar decisiones informadas sobre las medidas de mitigación y control necesarias para salvaguardar la seguridad de la información y mantener una reputación sólida.

LOS CRITERIOS DE IMPACTO DEL RIESGO

Los criterios de impacto del riesgo son parámetros específicos que se definen en función del grado de daño o de los costos que la E.S.E. UNA podría experimentar como consecuencia de un evento de seguridad de la información. Estos criterios consideran diversos aspectos clave para evaluar el impacto potencial:

- Nivel de Clasificación de los Activos de Información de los Procesos: Este criterio se enfoca en la importancia y clasificación de los activos de información asociados a los procesos de la E.S.E. UNA. La pérdida o compromiso de información clasificada conlleva un mayor impacto en la seguridad.
- Brechas en la Seguridad de la Información: Se evalúa el impacto de las brechas en la seguridad, como la pérdida de confidencialidad, integridad o disponibilidad de la información. Estas brechas pueden tener consecuencias significativas en la operación y reputación de la E.S.E. UNA.
- Operaciones Deterioradas: Se considera el impacto en las operaciones cotidianas de la E.S.E. UNA. Interrupciones o deterioro en las operaciones pueden afectar la eficiencia y la capacidad de cumplir con sus funciones.
- Pérdida de la Misión y del Valor Financiero: Este criterio evalúa cómo un evento de seguridad podría comprometer la misión de la entidad y afectar su valor financiero. La pérdida de la misión puede tener consecuencias a largo plazo en la identidad y objetivos de la organización.

- Alteración de Planes y Fechas Límites: Se examina cómo un evento de seguridad podría alterar los planes estratégicos y las fechas límites establecidas por la entidad. Cambios en la planificación pueden tener implicaciones en la consecución de objetivos.
- Daños para la Reputación: Este criterio evalúa el impacto en la reputación de la E.S.E. UNA. Daños a la reputación pueden resultar en pérdida de confianza por parte de clientes, socios y partes interesadas, afectando las relaciones comerciales y la percepción pública.
- Incumplimiento de Requisitos Legales: Se considera el impacto de un evento de seguridad en el cumplimiento de requisitos legales y reglamentarios. El incumplimiento puede dar lugar a sanciones legales y multas, afectando la posición legal de la entidad.

La definición precisa de estos criterios proporciona una base sólida para la evaluación del impacto del riesgo, permitiendo a la E.S.E UNA tomar decisiones informadas en la gestión de la seguridad de la información y la mitigación de posibles consecuencias adversas.

LOS CRITERIOS DE ACEPTACIÓN DEL RIESGO

Son pautas establecidas para determinar en qué condiciones un riesgo puede ser aceptado sin implementar medidas adicionales de mitigación. Estos criterios pueden variar según la expectativa de duración del riesgo y pueden incluir diversos elementos clave:

CRITERIOS GENERALES:

Estos criterios abordan aspectos generales relacionados con la naturaleza y magnitud del riesgo. Pueden incluir consideraciones sobre la probabilidad de ocurrencia, el impacto potencial y la tolerancia de la organización hacia ciertos niveles de riesgo.

Aspectos Legales y Reglamentarios:

Los criterios de aceptación del riesgo pueden estar influenciados por el cumplimiento de requisitos legales y reglamentarios. Si un riesgo no contraviene normativas establecidas, podría ser aceptado en ciertos contextos.

Operaciones:

Se considera la viabilidad de las operaciones frente al riesgo. Si un riesgo no impide de manera significativa las operaciones diarias y no afecta críticamente los procesos clave, podría ser aceptado.

Tecnología:

Los criterios relacionados con la tecnología abordan la capacidad de los sistemas y tecnologías de la organización para mitigar o gestionar el riesgo. Si los sistemas existentes pueden tolerar o compensar el riesgo de manera efectiva, podría ser aceptado.

Finanzas:

Los aspectos financieros son esenciales en la toma de decisiones sobre la aceptación del riesgo. Se evalúa si la organización tiene recursos financieros para mitigar el riesgo o si es más viable aceptarlo sin incurrir en costos significativos.

Factores Sociales y Humanitarios:

Este criterio considera los aspectos sociales y humanitarios relacionados con la aceptación del riesgo. Puede incluir la evaluación de posibles impactos negativos en la comunidad, en la fuerza laboral y en otros grupos de interés.

Este criterios proporciona a la E.S.E. UNA, una guía clara para decidir cuándo un riesgo puede ser aceptado sin la necesidad de implementar medidas adicionales de mitigación.

VALORACIÓN DEL RIESGO:

En el proceso de valoración del riesgo, se parte del contexto estratégico de la entidad, que implica reconocer tanto las situaciones de riesgo internas como externas. Se procede a la identificación y evaluación de riesgos, teniendo en cuenta diversas variables como los agentes generadores, las causas y los efectos, entre otros factores relevantes. La calificación de los riesgos se lleva a cabo después de este análisis detallado.

Al considerar los factores internos y externos, se determinan los agentes generadores de riesgo en el ámbito de la seguridad y privacidad de la información. Se analizan las causas subyacentes y las posibles consecuencias, que pueden incluir pérdida, daño, perjuicio o detrimento. Este enfoque integral permite una comprensión profunda de los riesgos asociados, lo que facilita la toma de decisiones informadas y la implementación de medidas adecuadas para gestionar y mitigar dichos riesgos.

A. IDENTIFICACIÓN DEL RIESGO: La identificación del riesgo tiene como objetivo principal discernir los posibles eventos que podrían ocasionar una pérdida potencial. Este proceso busca comprender en detalle el cómo, dónde y por qué podría materializarse dicha pérdida. En esencia, se trata de anticipar y reconocer cualquier circunstancia o evento que tenga el potencial de generar consecuencias adversas para la organización. La identificación del riesgo implica un análisis exhaustivo para determinar escenarios posibles, sus causas subyacentes y la naturaleza de las pérdidas que podrían derivarse, lo que proporciona una base sólida para la gestión y mitigación efectiva de los riesgos identificados.
B. IDENTIFICACIÓN DE LAS AMENAZAS: implica reconocer y evaluar las posibles fuentes de peligro que podrían causar daños a los activos de la E.S.E.UNA, incluyendo información, procesos y sistemas. Estas amenazas pueden surgir tanto de eventos naturales como de acciones humanas, y pueden ser accidentales o intencionales. Es crucial identificar todos los posibles orígenes de amenazas, ya sean accidentales o deliberados, para tener una comprensión completa de los riesgos a los que se enfrenta la entidad. Es recomendable clasificar las amenazas de manera genérica y por tipo, por ejemplo, acciones no autorizadas, daño físico o fallas técnicas.

C. IDENTIFICACIÓN DE LOS ACTIVOS: Se refiere al proceso de reconocer y catalogar todos los elementos de valor para la E.S.E. UNA. En el contexto de la seguridad de la información, según la norma ISO 27001:2013, un activo es cualquier cosa que posea valor y requiera protección. Esta identificación debe llevarse a cabo con un nivel de detalle suficiente para proporcionar la información necesaria para la evaluación de riesgos.

D. IDENTIFICACIÓN DE LOS CONTROLES EXISTENTES: La identificación de controles existentes se refiere al proceso de reconocer y evaluar las medidas de seguridad y salvaguardias ya implementadas en una entidad. Este procedimiento busca evitar redundancias y gastos innecesarios, como la duplicidad de controles, al tiempo que garantiza la eficacia de los controles identificados. Además de simplemente identificarlos, se recomienda realizar una verificación para asegurarse de que los controles existentes funcionen correctamente.

E. IDENTIFICACIÓN DE LAS VULNERABILIDADES: La identificación de vulnerabilidades es el proceso sistemático de reconocer y catalogar debilidades, fallos o puntos susceptibles en los sistemas, procesos, procedimientos, recursos humanos y tecnológicos de una organización que podrían ser explotados por amenazas para causar daño o pérdida. Este proceso implica analizar exhaustivamente diversos aspectos, como la infraestructura tecnológica, las prácticas organizativas, las configuraciones de sistemas y la capacitación del personal, con el objetivo de identificar áreas donde la seguridad puede ser comprometida.

- ✓ Organización.
- ✓ Procesos y procedimientos.
- ✓ Rutinas de gestión.
- ✓ Personal
- ✓ Ambiente físico
- ✓ Configuración del sistema de información.
- ✓ Hardware, software y equipos de comunicaciones.
- ✓ Dependencia de partes externas.

F. IDENTIFICACIÓN DE LAS CONSECUENCIAS: La identificación de las consecuencias implica un proceso integral que requiere dos elementos clave: una lista de activos de información y su relación con los procesos de la entidad, así como una lista de amenazas y vulnerabilidades en relación con esos activos y su relevancia. Es crucial reconocer que las consecuencias pueden abarcar desde la pérdida de eficacia y condiciones adversas de operación hasta daños en la reputación. En este proceso, se deben identificar las consecuencias operativas de los posibles escenarios de incidentes, considerando factores como el tiempo necesario para la investigación y reparación, la pérdida de tiempo operacional, oportunidades, riesgos para la salud y seguridad, costos financieros y el impacto en la imagen y reputación de la entidad. Esta evaluación detallada permite una comprensión holística de las repercusiones potenciales, facilitando así la implementación de medidas preventivas y correctivas efectivas.

En un plan de tratamiento de riesgo y seguridad de la información para un E.S.E. UNA, se pueden proponer diversas actividades para mitigar, transferir, aceptar o evitar los riesgos identificados. Aquí tienes una enumeración de posibles actividades a considerar:

ANALISIS DE RIESGOS

El análisis de riesgos es un proceso detallado que implica evaluar las posibles consecuencias o efectos derivados de la ocurrencia de riesgos, tomando en consideración los objetivos específicos de la E.S.E. Estas consecuencias pueden manifestarse en diversas formas, ya sea afectando a personas, bienes materiales o aspectos intangibles como la imagen y el prestigio corporativo. Durante este análisis, se examinan minuciosamente los posibles escenarios de riesgo y se cuantifican sus impactos en relación con los objetivos institucionales y los activos críticos. Este enfoque permite una comprensión más profunda de las repercusiones potenciales, lo que facilita la toma de decisiones informadas sobre la gestión y mitigación de riesgos para garantizar la continuidad operativa y la protección integral de la E.S.E. UNA.

Para realizar el análisis se utiliza las siguientes tablas para evaluar la probabilidad y el impacto:

CRITERIOS PARA CLASIFICAR LA PROBABILIDAD DE OCURRENCIA DEL RIESGO

CALIFICACIÓN	VARIABLE
REMOTA	Improbable que ocurra (No ha ocurrido en los últimos 5 años).
RARO	Posible que ocurra en algún momento (puede ocurrir al menos una vez en los últimos 5 años).
OCASIONAL	Probablemente ocurrirá (puede suceder al menos una vez en los últimos dos años).
FRECUENTE	Probablemente ocurrirá en la mayoría de las circunstancias (Al menos una vez en el último año).
CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias (más de una vez al año).

CRITERIOS PARA LA CALIFICACIÓN DEL IMPACTO DEL RIESGO

CALIFICACIÓN	VARIABLE
INSIGNIFICANTE	Las consecuencias de los riesgos, si ocurren no afectan a ningún proceso de la E.S.E. UNA.
MENOR	Las consecuencias de los riesgos, si ocurren, afectan levemente a la E.S.E.y pueden pasar desapercibidas para el paciente y no afectan la prestación del servicio ni la imagen institucional. En equipos o instalaciones daños por cuantía menor a 150 SMLMV.
MODERADO	Las consecuencias de los riesgos pueden afectar parcialmente los procesos y servicios del E.S.E. UNA, pero las pérdidas y daños son menores y no afectan la imagen institucional. En los pacientes puede aumentar la estancia o el nivel de complejidad de cuidados para 1 o 2 pacientes; en los visitantes puede requerirse atención sin hospitalización para 1 o 2 de ellos; en lo personal pérdida de tiempo y restricciones por enfermedad o lesiones. En equipos o instalaciones daños por cuantía de 150 a 450SMLMV.
MAYOR	Las consecuencias de los riesgos pueden afectar de manera importante los procesos y servicios del E.S.E. UNA y afectarse igualmente la imagen institucional. En los pacientes puede producirse discapacidad, desfiguramiento, requerir intervención quirúrgica y aumento de la estancia o del nivel de complejidad en cuidados para 3 o más pacientes; en los visitantes puede requerirse hospitalización para 1 o 2 de ellos; en la personal hospitalización de 1 o 2 de ellos. En equipos o instalaciones daños por cuantía de 450 a 1500 SMLMV
CATASTROFICO	Las consecuencias pueden afectar totalmente a la E.S.E UNA produciendo daños recuperables y afectarse la imagen institucional de manera grave El resultado en pacientes puede ser muerte o discapacidad grave, suicidio, violación, reacción-hemofílica post- transfusional, cirugía en sitio equivocado, rapto de niños, entrega de niños a familia equivocada; en visitantes puede

	producirse muerte o requerirse hospitalización para más de 3 personas; en el personal puede producir muerte u hospitalización de 3 o más personas. En equipos o instalaciones daños por cuantía superior a 1500 SMLMV.

DETERMINACIÓN DE ÁREAS DE RIESGO INFORMATICO

La identificación de áreas de riesgo informático en la E.S.E. Universitaria del Atlántico se centrará en las tecnologías de información y comunicaciones, esenciales para el cumplimiento de su misión. Las áreas principales de riesgo incluyen las bases de datos, servicios de información y administrativos, y la seguridad informática (comunicaciones), que están estrechamente interrelacionadas.

AMENAZA	VULNERABILIDAD
MEDIO AMBIENTE E INFRAESTRUCTURA	Controles de acceso a centros de datos inadecuados.
	Suministro eléctrico inestable.
	Desastres naturales.
	Desastres causados por el hombre.
	Inadecuado sistema de prevención de atención de desastres.
RECURSO HUMANO	Contratación inadecuada.
	Ausentismo.
	Roles y responsabilidades inadecuados – Falta de conciencia alrededor de la seguridad informática.
	Falta de capacitación.
	Falta de procedimientos oficiales
	Desastres ocasionados por el hombre
SOFTWARE	Falta de conciencia alrededor de la seguridad informática.
	Software malicioso.
	Exposición de contraseñas de acceso a servicios informáticos
	Exposición de contraseñas de acceso a servicios informáticos
HARDWARE	Daño
	Degradación
	Plan de mantenimiento inapropiado.
	Suministro eléctrico inestable.
COMUNICACIONES	Falta de esquemas de alta disponibilidad (respaldo)
	Administración de red inadecuada
DATOS (INFORMACIÓN)	Inadecuada clasificación de activos
	Software malicioso
	Protección inadecuada de bases de datos.
	Falta de plan de procedimientos y software de respaldo

SISTEMAS Y SERVICIOS INFORMATICOS CRÍTICOS

Los riesgos asociados al uso de tecnologías de información y comunicaciones que podrían impactar de manera total o parcial en el adecuado funcionamiento de los sistemas y servicios informáticos de la E.S.E. Universitaria del Atlántico resaltan la necesidad de identificar los procesos críticos dentro de la entidad. Este enfoque implica reconocer las operaciones y funciones más vitales para el E.S.E. UNA, con el propósito de establecer procedimientos alternos que aseguren la continuidad en la operación informática ante posibles interrupciones. La identificación de estos procesos críticos permite implementar medidas específicas de resiliencia y contingencia, garantizando que, incluso en situaciones adversas, la entidad pueda mantener sus funciones esenciales y preservar la integridad de los servicios informáticos críticos.

EVALUACIÓN DEL RIESGO

La evaluación de riesgos constituye la fase final del proceso y se lleva a cabo de manera que se pueda determinar la probabilidad de ocurrencia y el impacto que un riesgo podría tener sobre las operaciones de la E.S.E. UNA. Con el propósito de facilitar la calificación y evaluación de los riesgos, se utiliza una matriz que aborda un análisis cualitativo. Esta matriz proporciona una representación visual de la magnitud de las posibles consecuencias (impacto) y la probabilidad de que ocurran (probabilidad). Al emplear este enfoque, se logra una comprensión más clara y estructurada de la importancia relativa de los riesgos, permitiendo una toma de decisiones informada para priorizar la gestión y mitigación de los riesgos identificados.

		IMPACTO *¿Qué tan severos serían los resultados si ocurriera el riesgo?*				
PROBABILIDAD ¿Cuál es la probabilidad de que ocurra el riesgo?		**INSIGNIFICANTE**	**MENOR**	**MODERADO**	**ALTO**	**CATASTRÓFICO**
	CASI SEGURO	**A**	**A**	**E**	**E**	**E**
	FRECUENTE	**M**	**A**	**A**	**E**	**E**
	OCASIONAL	**B**	**M**	**A**	**E**	**E**
	RARO	**B**	**B**	**M**	**A**	**E**
	REMOTA	**B**	**B**	**M**	**A**	**A**

B: Zona de riesgo baja: Asumir el riesgo

M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo

A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir

E: Zona de riesgo extrema: Reducir el riesgo, evitar, compartir o transferir

TRATAMIENTO DE RIESGOS

El tratamiento de riesgos es el proceso integral que sigue a la identificación y análisis de riesgos, y se centra en la toma de decisiones para mitigar o gestionar los riesgos identificados. En este contexto, se lleva a cabo un análisis detallado de las posibles acciones a emprender, asegurándose de que sean factibles y efectivas. Estas acciones pueden incluir la implementación de políticas, la definición de estándares, la optimización de procesos y procedimientos, así como cambios físicos, entre otras medidas. La esencia del tratamiento de riesgos radica en la capacidad de tomar decisiones informadas y estratégicas basadas en los resultados obtenidos durante la identificación y análisis de riesgos. El objetivo final es reducir la probabilidad de ocurrencia o el impacto de los riesgos, garantizando así la seguridad y la continuidad efectiva de las operaciones de la entidad.

ZONAS O NIVELES DE CRITICIDAD E INTERVENCIÓN DEL RIESGO		TRATAMIENTO
RIESGO BAJO	Dada su baja probabilidad de presentación, es posible asumir el riesgo, pero deben planearse acciones para reducirlo en caso que se presente.	Asumir el riesgo
RIESGO MODERADO	Evaluada la probabilidad e impacto es posible asumir el riesgo, pero siempre acompañado de acciones para reducirlo y evitarlo en lo posible.	Asumir el riesgo, reducir el riesgo
RIESGO ALTO	En esta zona de riesgo alta debe siempre evitar, reducir, compartir o transferir el riesgo.	Reducir el riesgo, evitar, compartir o transferir
RIESGO EXTREMO	En esta zona de riesgo extrema debe siempre y de manera simultánea: evitarse el riesgo, reducirlo y compartir o transferir el riesgo. Los puntos de control deben ser más estrictos.	Reducir el riesgo, evitar, compartir o transferir.

IMPACTO DE CONFIDENCIALIDAD EN LA INFORMACIÓN:

El impacto de confidencialidad de la información se refiere a la pérdida o revelación de la misma. Cuando se habla de información reservada institucional se hace alusión a aquella que por la razón de ser de la E.S.E. solo puede ser conocida y difundida al interior de la misma; así mismo, la sensibilidad de la información depende de la importancia que esta tenga para el desarrollo de la misión de la entidad.

NIVEL	CONCEPTO
1	Personal
2	Grupo de trabajo
3	Relativa al proceso
4	Institucional
5	Estratégica

IMPACTO DE CREDIBILIDAD O IMAGEN:

El impacto de credibilidad se refiere a la pérdida de la misma frente a diferentes actores sociales o dentro de la entidad.

NIVEL	CONCEPTO
1	Grupo de funcionarios
2	Todos los funcionarios
3	Usuarios ciudad
4	Usuarios Región
5	Usuarios País

IMPACTO LEGAL:

El impacto legal se relaciona con las consecuencias legales para una entidad, determinadas por los riesgos relacionados con el incumplimiento en su función administrativa, ejecución presupuestal y normatividad aplicable.

NIVEL	CONCEPTO
1	Multas
2	Demandas
3	Investigación disciplinaria
4	Investigación fiscal
5	Intervención – Sanción.

IMPACTO OPERATIVO:

El impacto operativo aplica en la mayoría de las entidades para los procesos clasificados como de apoyo, ya que sus riesgos pueden afectar el normal desarrollo de otros procesos.

NIVEL	CONCEPTO
1	Ajuste de una actividad concreta.
2	Cambios en los procedimientos.
3	Cambios en la interacción de los procesos.
4	Intermitencia en los servicios.
5	Paro total de los procesos.

Teniendo en cuenta que para un proceso es posible analizar más de un impacto, se pueden ir agrupando en el siguiente cuadro, en el cual se establecen concretamente.

TIPO DE IMPACTO	IMAGEN
INSIGNIFICANTE 1	Se afectó al grupo de funcionarios del proceso
MENOR 2	Se afectó a todos los funcionarios de la entidad.
MODERADO 3	Se afectó a los usuarios locales.
MAYOR 4	Se afectó a los usuarios locales y regionales.
CATASTRÓFICO 5	Se afectó a los usuarios en el orden nacional

MONITOREO Y REVISIÓN

El monitoreo y revisión son componentes esenciales en la gestión efectiva de riesgos, y su implementación seguirá un proceso estructurado en la E.S.E. Universitaria del Atlántico. La supervisión iniciará con el responsable del proceso, que puede ser el Gerente o la Oficina Asesora de Planeación, quienes realizará el seguimiento inicial para asegurar la ejecución de las acciones planificadas y evaluar la eficiencia de su implementación.

En un segundo momento, el subgerente, encargado de los procesos asistenciales, administrativos y financieros, realiza un seguimiento adicional. Este enfoque jerárquico garantiza una cobertura completa de los distintos aspectos de la entidad.

La Oficina de Control Interno desempeñará un papel clave al comunicar y presentar los resultados y propuestas de mejora tras la evaluación. Se llevará a cabo al menos semestralmente, y se centrará en detectar situaciones que requieran tratamiento o ajuste. Además, cada responsable de proceso realiza autoevaluaciones periódicas para determinar la efectividad de los controles implementados y minimizar los riesgos. Simultáneamente, la Oficina de Control Interno emite su informe de evaluación de riesgos y controles de segundo orden.

Este enfoque estructurado y jerárquico garantizará una supervisión continua y exhaustiva de la gestión de riesgos, facilitando la identificación temprana de posibles problemas y permitiendo la implementación proactiva de mejoras para fortalecer la resiliencia de la E.S.E. UNA frente a posibles riesgos.

DERECHOS DE AUTOR

En la implementación del Modelo de Seguridad y Privacidad de la Información en la ESE UNA, nos referimos a que todas las menciones y referencias a los documentos de este modelo se realizan siguiendo las indicaciones proporcionadas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Estas indicaciones son parte de la estrategia de Gobierno en Línea y tienen como objetivo guiar la implementación de prácticas de seguridad y privacidad de la información en la entidad.

Adicionalmente, cuando hacemos referencia a las políticas, definiciones u otro contenido relacionado, estamos hablando de seguir las pautas establecidas en la norma técnica colombiana NTC ISO/IEC 27001 y la norma ISO 27005, ambas actualmente en vigencia. Además, es importante señalar que algunos anexos relacionados con estos estándares tienen derechos reservados por parte de ISO/ICONTEC, lo que significa que se deben respetar estos derechos de propiedad intelectual al utilizar o hacer referencia a dichos anexos. En resumen, se trata de seguir lineamientos específicos y respetar la propiedad intelectual al implementar las medidas de seguridad y privacidad de la información en la ESE UNA.

El PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN debe ser adaptado a la realidad específica de la E.S.E. Universitaria del Atlántico, teniendo en cuenta sus activos, amenazas y vulnerabilidades particulares. Además, se solicita la participación activa de todas las partes interesadas en el proceso para asegurar una implementación efectiva y sostenible.

Las actividades a desarrollar dentro del Plan de Tratamiento de riesgos y seguridad de la información de la E.S.E. Universitaria del Atlántico para el año 2024 son:

- Identificación de Activos de Información
- Identificación de información crítica y sensible.
- Evaluación de la ubicación y formato de almacenamiento.
- Clasificación de la información según su importancia.

E.S.E. UNIVERSITARIA DEL ATLÁNTICO

MATRIZ DE IDENTIFICACIÓN E ACTIVOS DE INFORMACIÓN

DIRECCIÓN TICS	FEBRERO								MARZO								ABRIL									MAYO									JUNIO								JULIO										AGOSTO							
	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	AY	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M
ÁREAS ADMINISTRATIVAS	5	7	12	14	19	21	#	#	4	6	11	13	18	#	#	#	1	3	8	10	15	17	#	#	#	1	6	8	13	15	#	#	#	#	3	5	10	12	17	19	#	#	1	3	8	10	15	17	#	#	#	31	5	7	12	14	19	21	#	#
SISTEMAS	X	X																																																										
DIRECCIÓN ADMINISTRATIVA			X	X																																																								
RECURSOS FÍSICOS					X	X																																																						
MANTENIMIENTO							X	X																																																				
ALMACEN									X	X																																																		
BIOMÉDICO JEFE											X	X																																														
ESTADÍSTICA													X	X																																												
ACTIVOS FIJOS															X	X																																										
SUBGERECIA CORPORATIVA																	X	X																																								
DIRECCIÓN FINANCIERA																			X	X																																						
ADMISIONES																					X	X																																				
AUTORIZACIONES																							X	X																																		
CARTERA																									X	X																																
CONTABILIDAD																											X	X																														
TESORERIA																													X	X																												
PRESUPUESTO																															X	X																										
FACTURACIÓN																																	X	X																								
GESTIÓN COMERCIAL																																			X	X																						
TALENTO HUMANO																																					X	X																				
CONTRATACIÓN																																							X	X																		
JURÍDICA																																									X	X																
DIRECCIÓN PLANEACIÓN																																											X	X														
COMUNICACIONES																																													X	X												
CONTROL INTERNO																																															X	X										
CONTROL DISCIPLINARIO																																																	X	X								
GARANTÍA DE LA CALIDAD																																																			X	X						
GERENCIA - DIRECCIONES TÉCNICAS																																																					X	X				
DOCENCIA																																																							X	X		
REFERENCIA Y CONTRAREFERENCIA																																																									X	X		

E.S.E. UNIVERSITARIA DEL ATLÁNTICO

MATRIZ DE IDENTIFICACIÓN E ACTIVOS DE INFORMACIÓN

DIRECCIÓN TICS	AGOSTO								SEPTIEMBRE									OCTUBRE									NOVIEMBRE								DICIEMBRE								
	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L	M	L
ÁREAS ASISTENCIALES	5	7	12	14	19	21	26	28	2	4	9	11	16	18	23	25	30	2	7	9	14	16	21	23	28	30	4	6	11	13	18	20	25	27	2	4	9	11	16	18	23	25	30
SUBGERENCIA CIENTÍFICA	■	■																																									
FARMACIA			■	■																																							
LABORATORIO					■	■																																					
NUTRICIÓN							■	■																																			
SIAU									■	■																																	
TRABAJO SOCIAL											■	■																															
IMAGENOLOGÍA													■	■																													
CITAS MEDICAS														■	■																												
CONSULTA ESPECIALIZADA														■	■																												
CONSULTA EXTERNA																■	■																										
HOSPITALIZACIÓN MEDICINA INTERNA																		■	■																								
HOSPITALIZACIÓN GINECOLOGÍA																				■	■																						
HOSPITALIZACIÓN MENTAL																						■	■																				
HOSPITALIZACIÓN NUEVA EPS																								■	■																		
HOSPITALIZACIÓN POLIVALENTE																										■	■																
COORDINACIÓN UCI																												■	■														
HOSPITALIZACIÓN UCI																														■	■												
HOSPITALIZACIÓN UCI NEONATAL																																■	■										
URGENCIAS																																		■	■								
QUIROFANOS																																				■	■						
APOYO TERAPEUTICO																																						■	■				
SERVICIOS AMBULATORIOS																																								■	■		
SERVICIOS CONEXOS																																										■	■

E.S.E. UNIVERSITARIA DEL ATLÁNTICO

Identificación del Activo de Información (Ley 594 de 2000 - Ley 1712 de 2014 - Decreto 103 de 2015 - Decreto 1080 de 2015 - Iso 27001:2013 - MIG)

Identificador	0	Tipo	Oficina	Serie Documental	Subserie Documental	Nombre	Descripción	Nombre del Responsable de la Producción de la Información (Propietari	Fecha de Generación de la Información	Nombre del Responsable de la Información (Custodio del Activo)	Fecha de Ingreso del Activo al Archivo	Tipo de Macroproceso	Macroproceso	Proceso	Documento MIG	Código Documento MIG	Norma, Ley o Función que lo Justifica	Origen	Soporte del Registro	Medio de Conservación	Formato	Idioma	FC

Valoración del Activo (Iso 27001:2013)								Índice de Información Clasificada y Reservada (Decreto 103 de 2015)					
Confidencialidad	FI	Integridad	FD	Disponibilidad	Criticidad del Activo	Información Publicada	Lugar de Consulta o Ubicación	Objetivo legítimo de la Excepción	Fundamento Constitucional o Legal	Fundamento Jurídico de la Excepción	Excepción Total o Parcial	Fecha de Calificación DD/MM/AAAA	Tiempo que Cobija la Clasificación

Protección de Datos Personales (Bases de Datos - Ley 1581 de 2012)					Datos Abiertos					
¿Contiene Datos Personales ?	Tipo de Datos Personales	Finalidad de la Recolección de los Datos Personales	Cuenta con las Autorizaciones para el Tratamiento de los Datos	¿Existe Transferencia Internacional de Datos Personales ?	¿Es un Conjunto de Datos Estratégico ?	¿Es un Dato Abierto?	Tipo Clasificación de Dato Publicado	URL de Publicación en Datos.gov.co	Cobertura Geográfica	Tipo de Información

CLASIFICACIÓN VALORACIÓN

VALOR	CONFIDENCIALIDAD
ALTO	**Pública Reservada / Confidencial:** Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica. Por lo tanto, cuando un activo de información realice tratamiento de datos personales privados o sensibles el activo de Información deberá ser calificado como activo de información pública confidencial (ALTO).
MEDIO	**Pública Clasificada / Uso Interno**: Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario. Por lo tanto, cuando un activo de información realice tratamiento de datos personales semiprivados, el activo de Información deberá ser calificado por lo menos como un activo de información pública de uso interno (MEDIO).
BAJO	**Pública / Pública** : Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
SIN CLASIFICAR	**SIN CLASIFICAR**: Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de Información Pública Reservada. (Alta).
VALOR	**INTEGRIDAD**
ALTO	**ALTO**: información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones o generar pérdidas de imagen severas de la Entidad.
MEDIO	**MEDIO**: información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado para la Entidad.
BAJO	**BAJO**: información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la Entidad o entes externos.
SIN CLASIFICAR	**SIN CLASIFICAR**: Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.
VALOR	**DISPONIBILIDAD**
ALTO	**ALTO**: La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.

MEDIO	**MEDIO**: La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
BAJO	**BAJO**: La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
SIN CLASIFICAR	**SIN CLASIFICAR**: Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

TIPO DE ACTIVOS	DESCRIPCIÓN
Bases de Datos	Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso, puede ser utilizada en un formato de motor ya sea SQL, SQL Server, MySQL o en formato Excel. Ejemplos: Bases de datos con información personal o con datos relevante para algún proceso (bases de datos de nóminas, Base de datos Aprendices, Listado de proveedores, estados financieros) entre otros.
Datos / Información	Que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos. Ejemplo: Copias de Respaldo, Ficheros, Datos de Gestión Interna, Datos de Configuración, Credenciales (Contraseñas), Datos de Validación de Credenciales (Autenticación), Datos de Control de Acceso, Registros de Actividad (Log), Matrices de Roles y Privilegios, Código Fuente, Código Ejecutable, Datos de Prueba, Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, formatos o formularios físicos o digitales.
Equipos Auxiliares	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos. Ejemplo: Fuentes de alimentación, generadores eléctricos, equipos de climatización, sistemas de alimentación ininterrumpida (UPS), cableado, cable eléctrico, fibra óptica, equipos de destrucción de soportes de información, mobiliarios, armarios, cajas fuertes.
Hardware / Infraestructura	Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la entidad, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. Ejemplo: Servidores (host), Equipos de Escritorio (Pc), Equipos Portátiles (Laptop), Dispositivos Móviles, Equipos de Respaldo, Periféricos, Dispositivos Criptográficos, Dispositivos Biométricos, Servidores de Impresión,

	Impresoras, Escáneres, Equipos Virtuales (host), Soporte de la Red (Network), Módems, Concentradores, Conmutadores (switch), Encaminadores (router), Pasarelas (bridge), Firewall, Central Telefónica, Telefonía IP, Access Point.
Instalaciones	Lugares donde albergan los sistemas de información y comunicaciones.
Personas	Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Programadores, Contratistas, Proveedores.
Redes de Comunicaciones	Infraestructuras dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro. Ejemplo: Red Telefónica, Red Inalámbrica, Telefonía Móvil, Satelital, Red Local (LAN), Red Metropolitana (MAN), Internet, Radio Comunicaciones, Punto a Punto, ADSL, Red Digital (RDSI).
Servicios	Funciones que permiten suplir una necesidad de los usuarios del servicio (internos o externos) Ejemplo: Página Web, Correo Electrónico, Acceso Remoto, almacenamiento de ficheros, transferencia de ficheros, intercambio electrónico de datos, Gestión de Identidades (altas y bajas de usuarios del sistema), Gestión de Privilegios, Intercambio electrónico de datos, PKI (Infraestructura de Clave Pública). o servicios relacionados con la misión de la Entidad, servicios relacionados con los prestados por la Entidad hacia los grupos de valor, servicios relacionados para el desarrollo de las funciones de grupos de interés
Software / Aplicaciones Informáticas	Que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. Ejemplo: Aquellos utilizados para la enseñanza, para el desarrollo de aplicaciones, para la gestión o administración de bases de datos, para la gestión o administración de documentos, para la gestión del correo electrónico, para la navegación web, para el desarrollo de aplicaciones propias, para la gestión de respaldos de información, para la prevención de virus o infecciones informáticas, para conexiones o trabajos remotos, entre otros.
Soportes de Información	Dispositivos físicos o electrónicos que permiten almacenar información de forma permanente o durante largos periodos de tiempo y que posteriormente permiten recuperar la información contenida en ellos. Ejemplo: Discos, Discos Virtuales, Almacenamiento en Red (san), Memorias USB, CDROM, DVD, Cinta Magnética (tape), Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso, Microfilmaciones.

DATOS GENERALES			
CAMPO	**DEFINICIÓN**	**INSTRUCTIVO**	**RESPONSABLE DE DILIGENCIAMIENTO**

DIRECCIÓN GENERAL / REGIONAL / CENTRO DE FORMACIÓN / SEDE	Permite identificar la dirección, oficina, territorial, y/o sede en la cual se está realizando el inventario y valoración de activos de información.	Diligencie el campo indicando la dirección, oficina, territorial o sede	Líder de proceso / Colaborador designado
LÍDER DE PROCESO O FUNCIONARIO DESIGNADO / CALIFICADO POR	Permite identificar la dirección, oficina, grupo, funcionario que realiza o con quien se realiza el inventario y valoración de activos de información.	Diligencie el campo indicando la dirección, oficina, grupo, funcionario	Líder de proceso / Colaborador designado
FECHA ÚLTIMA ACTUALIZACIÓN	Permite realizar el registro de la fecha en la cual se realizo el inventario y valoración de activos de información.	Diligencie la fecha en la que realizó la creación o actualización del inventario de activos	Líder de proceso / Colaborador designado
IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN			
CAMPO	**DEFINICIÓN**	**INSTRUCTIVO**	**RESPONSABLE DE DILIGENCIAMIENTO**
ID. ACTIVO	Permite realizar una asignación consecutiva de un identificador para cada activo que sea registrado como parte el inventario de activos de información.	El campo es automático y no se diligencia	Automático por herramienta
PROCESO	Permite Seleccionar a cual de los procesos definidos en el Mapa de procesos pertenece el activo de información. **[Opciones disponibles]** *Los procesos de la entidad*	Registre el nombre del proceso al cual pertenece el activo de información.	Líder de proceso / Colaborador designado
NOMBRE DEL ACTIVO DE INFORMACIÓN	Permite registrar el nombre a través del cual se puede hacer referencia al activo de información que este siendo identificado.	Registre el nombre a través del cual se identifica el activo de información.	Líder de proceso / Colaborador designado
DESCRIPCIÓN DEL ACTIVO DE INFORMACIÓN	Permite realizar el registro de una breve descripción o detalle que permite contextualizar o proporcionar más información sobre el activo de información. *Que es? Para que sirve? Que agrupa? A que hace referencia? Etc.*	Realice una breve descripción que ayude a contextualiza el activo de información que está registrando.	Líder de proceso / Colaborador designado
AÑO DE IDENTIFICACIÓN / ACTUALIZACIÓN	Registre el año de identificación o actualización del activo de información	Registre el año de identificación o actualización del activo de información	Líder de proceso / Colaborador designado
USUARIOS (TODA LA ENTIDAD / NOMBRE DEL CARGO / DEPENDENCIA / GRUPO / OFICINA)	Permite realizar el registro de quien(es) hace(n) uso del activo de información. Puede ser toda la entidad, direcciones, oficinas, grupos, cargos, roles, terceros, otras entidades, etc.	Registre si es toda la entidad, grupos, direcciones, oficinas, terceros, u otras entidades. Puede separar cada uno de ellos usando el carácter "/" sin comillas	Líder de proceso / Colaborador designado

PROPIETARIO (NOMBRE DEL CARGO / DEPENDENCIA / GRUPO / OFICINA)	Permite realizar el registro de quienes son los dueños o deciden sobre el activo de información. Quienes son aquellos que definen los controles, lo modifican, crean, cambian, ajustan, eliminan o transforman el activo de información. Puede ser toda la entidad, direcciones, oficinas, grupos, cargos, roles, terceros, otras entidades, etc.	Registre si es toda la entidad, direcciones, oficinas, grupos, cargos, roles, terceros, otras entidades, etc. Puede separar cada uno de ellos usando el carácter "/" sin comillas	Líder de proceso / Colaborador designado
CUSTODIO (NOMBRE DEL CARGO / DEPENDENCIA / GRUPO / OFICINA)	Permite realizar el registro de quienes aplican los controles que define el o los propietario(s), en relación almacenamiento, respaldo, accesos, permisos, etc. Puede ser toda la entidad, direcciones, oficinas, grupos, cargos, roles, terceros, otras entidades, etc.	Registre si es toda la entidad, direcciones, oficinas, grupos, cargos, roles, terceros, otras entidades, etc. Puede separar cada uno de ellos usando el carácter "/" sin comillas	Líder de proceso / Colaborador designado

TABLAS DE RETENCIÓN DOCUMENTAL			
CAMPO	**DEFINICIÓN**	**INSTRUCTIVO**	**RESPONSABLE DE DILIGENCIAMIENTO**
SERIE	Permite realizar el registro del nombre asignado en la tabla de retención documental para la serie. Ejemplo: *"ACTAS"*	Registre el nombre asignado en la tabla de retención documental para la serie. En caso de no contar con una clasificación documental, en este campo se registra la expresión "N/A" y se procede a revisar el cuadro de clasificación documental ya sea para la actualización o para la elaboración de la TRD, según corresponda.	Líder de proceso / Colaborador designado
SUBSERIE	Permite realizar el registro del nombre asignado en la tabla de retención documental para la subserie. Ejemplo: *"Actas de comisiones intersectoriales"*	Registrar el nombre asignado en la tabla de retención documental para la subserie. En caso de no contar con una clasificación documental, en este campo se registra la expresión "N/A" y se procede a revisar el cuadro de clasificación documental ya sea para la actualización o para la elaboración de la TRD, según corresponda.	Líder de proceso / Colaborador designado
TITULO DE LA INFORMACIÓN	Es el nombre asignado a la serie o subserie documental. Ejemplo: *"Acta de comité intersectorial"*	Registre el nombre que se le asigna al activo con el fin de identificar la información a la que hace referencia. En caso de no contar con un titulo registrar "N/A".	Líder de proceso / Colaborador designado
VALORACIÓN DEL ACTIVO			
CAMPO	**DEFINICIÓN**	**INSTRUCTIVO**	**RESPONSABLE DE DILIGENCIAMIENTO**
Tipo de Activo	Permite seleccionar la categoría a la cual pertenece el activo de información que estamos identificando. Puede conocer las diferentes categorías y su descripción en la pestaña "Tipo de Activos" de la matriz.	Seleccione la categoría a la cual pertenece el tipo de activo que esta identificando. Ej. [Documentos, archivos, formatos, guías, instructivos, actas] -> Datos / Información; [Equipos de computo de escritorio, portátiles, servidores, routers, switch] -> Hardware / Infraestructura	Líder de proceso / Colaborador designado
CRITICIDAD RESPECTO A LA CONFIDENCIALIDAD	Permite realizar la selección de la calificación asociada a la criticidad de la confidencialidad. Puede conocer los diferentes niveles de calificación y sus descripciones en la pestaña "Tipos de Activos"	Seleccione la calificación del la confidencialidad del activo de información según los establecidos en la pestaña "Calificación Valoración"	Líder de proceso / Colaborador designado

CRITICIDAD RESPECTO A LA INTEGRIDAD	Permite realizar la selección de la calificación asociada a la criticidad de la Integridad. Puede conocer los diferentes niveles de calificación y sus descripciones en la pestaña "Tipo de Activos"	Realice la calificación del la integridad del activo de información según los criterios suministrados y disponibles.	Líder de proceso / Colaborador designado
CRITICIDAD RESPECTO A LA DISPONIBILIDAD	Permite realizar la selección de la calificación asociada a la criticidad de la Disponibilidad. Puede conocer los diferentes niveles de calificación y sus descripciones en la pestaña "Tipo de Activos"	Realice la calificación del la disponibilidad del activo de información según los criterios suministrados y disponibles.	Líder de proceso / Colaborador designado
Valor del Activo para el proceso	Permite generar la valoración cualitativa del activo de acuerdo a la escala establecida y la selección realizada en el campo anterior	El campo es automático y no se diligencia	Cálculo automático
OBSERVACIONES	Permite realizar el registro de observaciones que se consideren necesarias con respecto al Activo de Información, puede anotarse también las razones por las cuales se realizaron las calificaciones, y qué se tuvo en cuenta para determinar las mismas.	Registre observaciones adicionales sobre el activo de información.	Líder de proceso / Colaborador designado

PROTECCION DE DATOS			
CAMPO	**DEFINICIÓN**	**INSTRUCTIVO**	**RESPONSABLE DE DILIGENCIAMIENTO**
El activo almacena o solicita Datos personales	Permite evaluar si el activo de información almacena o solicita datos personales. Ej. Datos de contacto, datos laborales, datos patrimoniales, datos académicos, entre otros. **[Opciones disponibles]** *Si; No*	Seleccione si el activo almacena o solicita datos personales.	Líder de proceso / Colaborador designado
Los datos almacenados o requeridos son públicos	Permite evaluar si el activo de información almacena o solicita datos personales de tipo publico, es decir, datos personales que la Entidad o las Leyes ha determinado expresamente como públicos. *Ej., correos laborales, nombre, cargos o roles, datos de contacto definidos como públicos, sentencias judiciales, documentos públicos, datos de gacetas o boletines, entre otros.* **[Opciones disponibles]** *Si; No*	Si seleccionó "Si" en el campo "**El activo almacena o solicita Datos personales**" este campo pasará de color gris a blanco con el fin de indicar que se ha habilitado y debe ser diligenciado. Si el campo se encuentra en blanco seleccione si los datos personales que almacena, solicita o recolecta son de tipo publico o no. *Si el campo se encuentra en color gris omita el diligenciamiento de este campo.*	Líder de proceso / Colaborador designado
Los datos almacenados o requeridos son Privados	Permite evaluar si el activo de información almacena o solicita datos personales de tipo privados, es decir, datos personales que por su naturaleza son datos que solo le interesan al titular y no deberían ser conocidos por terceros. *Ej. correo electrónico personal, teléfono, dirección de vivienda, datos laborales, nivel de escolaridad, sobre infracciones administrativas o penales, los datos administrados por algunas entidades como tributarias, financieras o de la seguridad social, fotografías, videos, y cualquier otro dato que referencien el estilo de vida de una persona.* **[Opciones disponibles]** *Si; No*	Si seleccionó "Si" en el campo "**El activo almacena o solicita Datos personales**" este campo pasará de color gris a blanco con el fin de indicar que se ha habilitado y debe ser diligenciado. Si el campo se encuentra en blanco seleccione si los datos personales que almacena, solicita o recolecta son de tipo privados o no. *Si el campo se encuentra en color gris omita el diligenciamiento de este campo.*	Líder de proceso / Colaborador designado

Los datos almacenados o requeridos son Semiprivados	Permite evaluar si el activo de información almacena o solicita datos personales de tipo privados, es decir, datos personales que por su naturaleza son datos que le interesan tanto al dueño de los datos como a terceros. *Ej. datos financiero y crediticio de actividad comercial o de servicios, datos de contacto personal, entre otros.* **[Opciones disponibles]** *Si; No*	Si seleccionó "Si" en el campo "**El activo almacena o solicita Datos personales**" este campo pasará de color gris a blanco con el fin de indicar que se ha habilitado y debe ser diligenciado. Si el campo se encuentra en blanco seleccione si los datos personales que almacena, solicita o recolecta son de tipo semiprivados o no. *Si el campo se encuentra en color gris omita el diligenciamiento de este campo.*	Líder de proceso / Colaborador designado
Los datos almacenados o requeridos son Sensibles	Permite evaluar si el activo de información almacena o solicita datos personales de tipo Sensibles, es decir, tipos de datos que, de acuerdo a la Ley 1581 de protección de datos colombiana, se han clasificado como sensibles, son de especial protección o pueden someter a discriminación. *Ej. origen étnico o racial, datos de salud, preferencia sexual, filiación política, religión, ideología, afiliación a sindicatos, organizaciones sociales, datos biométricos, de menores de edad, niños, niñas y adolescentes, entre otros.* **[Opciones disponibles]** *Si; No*	Si seleccionó "Si" en el campo "**El activo almacena o solicita Datos personales**" este campo pasará de color gris a blanco con el fin de indicar que se ha habilitado y debe ser diligenciado. Si el campo se encuentra en blanco seleccione si los datos personales que almacena, solicita o recolecta son de tipo sensible o no. *Si el campo se encuentra en color gris omita el diligenciamiento de este campo.*	Líder de proceso / Colaborador designado
Se debería validar la existencia de una autorización para el tratamiento de datos	Permite evaluar cual es el estado de autorización para el tratamiento o uso de los datos personales que están siendo almacenados, solicitados o requeridos en el activo de información **[Opciones disponibles]** *No requiere; Si requiere y no está definido; Si requiere y está definido*	Si seleccionó "Si" en el campo "**El activo almacena o solicita Datos personales**" este pasará de color gris a blanco con el fin de indicar que se ha habilitado y debe ser diligenciado. Si el campo se encuentra en blanco seleccione el estado de autorización para el tratamiento de datos. *Si el campo se encuentra en color gris omita el diligenciamiento de este campo.*	Líder de proceso / Colaborador designado

LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN			
CAMPO	**DEFINICIÓN**	**INSTRUCTIVO**	**RESPONSABLE DE DILIGENCIAMIENTO**
IDIOMA	Permite establecer en que Idioma, lengua o dialecto se encuentra o conserva la información del activo de información. **[Opciones disponibles]** *Español; Inglés; Español - Ingles; Otro*	Seleccione en que idioma se encuentra o conserva la información de acuerdo con las opciones disponibles. *Este campos solo se diligencia si la categoría seleccionada en el Tipo de Activo es "Datos / Información" o "Bases de datos".*	Líder de proceso / Colaborador designado

MEDIO DE CONSERVACIÓN Y/O SOPORTE	Permite establecer la manera en que se genera, crea, desarrolla o conserva el activo de información. **[Opciones disponibles]** ***Físico - Análogo:*** *si el documento de archivo - registro o activo de información se encuentra elaborado en soporte papel y cinta (video, casete, película, microfilm, entre otros).* ***Digital:*** *si el documento de archivo - registro o activo de información ha sido digitalizado o ha sufrido un proceso de conversión de una señal o soporte analógico a una representación digital (Archivo General de la Nación. Acuerdo 027 de 2006).* ***Electrónico:*** *si el documento de archivo - registro o activo de información es recibido, almacenado y comunicado se encuentra en medios electrónicos, y permanece en estos medios durante su ciclo vital (Archivo General de la Nación. Acuerdo 027 de 2006).* ***Hibrido Análogo Digital:*** *si el documento se encuentra en estos dos tipos de formatos* ***Hibrido Análogo Electrónico:*** *si el documento se encuentra en estos dos tipos de formatos*	Seleccione el medio de conservación del activo de información de acuerdo a las opciones disponibles. *Este campos solo se diligencia si la categoría seleccionada en el Tipo de Activo es "Datos / Información" o "Bases de datos".*	Líder de proceso / Colaborador designado
FORMATO VISUALIZACIÓN O CONSULTA	Permite establecer de que manera se suministraría la información del activo de información en caso que un ciudadano requiera visualizarla o consultarla. **[Opciones disponibles]** *Audio; Documento de Texto; Documento PDF; Presentación; Hoja de calculo; Imagen; Video; Otro; No aplica*	Seleccione el medio de visualización o consulta del activo de información de acuerdo a las opciones disponibles. *Este campos solo se diligencia si la categoría seleccionada en el Tipo de Activo es "Datos / Información" o "Bases de datos".*	Líder de proceso / Colaborador designado
INFORMACIÓN PUBLICADA O DISPONIBLE	Permite establecer como un ciudadano podría encontrar u obtener acceso a la información. **[Opciones disponibles]** *Publicada; Disponible a solicitud; No publicado o disponible*	Seleccione el cómo se podría encontrar u obtener acceso a la información de acuerdo a las opciones disponibles. *Este campos solo se diligencia si la categoría seleccionada en el Tipo de Activo es "Datos / Información" o "Bases de datos".*	Líder de proceso / Colaborador designado
FECHA DE GENERACIÓN DE LA INFORMACIÓN	Permite establecer la fecha desde la cual se genera o puede consultar la información.	Registre en formato DD/MM/AAAA la fecha desde la cual se genera o puede consultar la información. Si la fecha no es concreta o no se puede identificarla fácilmente puede: 1. Definir la fecha de acuerdo con lo establecido en tablas de retención documental para el activo; 2. Si la información del activo es generado, creado o expedido por una norma, tome la fecha de generación a partir de la fecha de expedición de la norma; o 3. Tome la fecha desde el 01/01/YYYY del año en curso. *Este campos solo se diligencia si la categoría seleccionada en el Tipo de Activo es "Datos / Información" o "Bases de datos".*	Líder de proceso / Colaborador designado
Nombre del responsable de la producción de la información	Corresponde al nombre del área, dependencia o unidad interna, o al nombre de la entidad externa que creó la información Permite establecer quien decide sobre el activo de información en términos de definir, controlar, modificar, crear, cambiar, ajustar, eliminar o transformar el activo de información. **[Opciones disponibles]** *Los procesos de la entidad*	Seleccione de los procesos disponibles cual sería el responsable de la producción de la información. En caso que el responsable no sea un proceso seleccione la opción "Definido Manualmente" para habilitar la siguiente columna donde podrá ser toda la entidad, direcciones, oficinas, grupos, cargos, roles, terceros, otras entidades, etc. *Este campos solo se diligencia si la categoría seleccionada en el Tipo de Activo es "Datos / Información" o "Bases de datos".*	Líder de proceso / Colaborador designado

Nombre del responsable de la producción de la información (digitado manualmente)	Corresponde al nombre del responsable del área, dependencia o unidad interna, o al nombre de la entidad externa que creó la información. Permite establecer quien decide sobre el activo de información en términos de definir, controlar, modificar, crear, cambiar, ajustar, eliminar o transformar el activo de información.	Registre el responsable de la producción de la información puede ser toda la entidad, direcciones, oficinas, grupos, cargos, roles, terceros, otras entidades, etc. *Este campos solo se diligencia si la categoría seleccionada en el Tipo de Activo es "Datos / Información" o "Bases de datos" y en el campo anterior es "Definido Manualmente"*	Líder de proceso / Colaborador designado
Nombre del custodio de la información:	Corresponde al nombre del área, dependencia o unidad encargada de la custodia o control de la información para efectos de permitir su acceso. Decreto 103/2015 **[Opciones disponibles]** *Los procesos de la entidad*	Seleccione de los procesos disponibles cual sería el responsable de la información. En caso que el responsable no sea un proceso seleccione la opción "Definido Manualmente" para habilitar la siguiente columna donde podrá ser toda la entidad, direcciones, oficinas, grupos, cargos, roles, terceros, otras entidades, etc. *Este campos solo se diligencia si la categoría seleccionada en el Tipo de Activo es "Datos / Información" o "Bases de datos".*	Líder de proceso / Colaborador designado
Nombre del custodio de la información (digitado manualmente)	Corresponde al nombre del área, dependencia o unidad encargada de la custodia o control de la información para efectos de permitir su acceso. Decreto 103/2015	Registre el responsable de la información puede ser toda la entidad, direcciones, oficinas, grupos, cargos, roles, terceros, otras entidades, etc. *Este campos solo se diligencia si la categoría seleccionada en el Tipo de Activo es "Datos / Información" o "Bases de datos" y en el campo anterior es "Definido Manualmente"*	Líder de proceso / Colaborador designado
CONDICIÓN LEGÍTIMA DE LA EXCEPCIÓN	Permite establecer cada una de las excepciones taxativas que se establecen en los artículos 18 y 19 de la Ley 1712. Es decir, las contenidas en los literales de los artículos mencionados. **[Opciones disponibles]** *Pone en riesgo la intimidad de las personas* *Pone en riesgo la vida, salud o seguridad de las personas* *Compromete secretos comerciales, industriales, profesionales* *Afectaría la defensa o seguridad nacional* *Afectaría la seguridad publica* *Afectaría o pone en riesgo las relaciones internacionales* *Compromete procesos de investigación de delitos o faltas disciplinarias* *Pone en riesgo procesos judiciales* *Compromete la administración efectiva de la justicia* *Pone en riesgo los derechos de la infancia o la adolescencia* *Afectaría o compromete la estabilidad macroeconómica o financiera del país* *Compromete o genera riesgo para la salud publica* *La información tiene tanto contenido publico como reservado o clasificado* *No existe excepción de acceso* *El activo de información no puede ser clasificado como información*	Seleccione las condiciones legitimas de excepción de acceso a la información del activo de información de acuerdo a las opciones disponibles. *Este campos solo se diligencia si la categoría seleccionada en el Tipo de Activo es "Datos / Información" o "Bases de datos".*	Líder de proceso / Colaborador designado

FUNDAMENTO CONSTITUCIONAL O LEGAL	Permite establecer registrar una norma, ley, decreto, circulares, normativas y aspecto legal que sustenta la condición legitima de la excepción. Ej.: *Ley de Protección de Datos (1581 de 2012), Ley de Transparencia (1712 de 2014), Ley 1448, etc...*	Registre el fundamento, norma, ley, decreto, circulares, normativas y aspecto legal que sustenta la condición legitima de la excepción. Este campos solo se diligencia si la categoría seleccionada en el Tipo de Activo es "Datos / Información" o "Bases de datos".	Líder de proceso / Colaborador designado
FUNDAMENTO JURIDICO DE LA EXCEPCIÓN	Establece la norma que sirve como fundamento jurídico para la clasificación o reserva de la información. Este campo se calcula de manera automática	El campo es automático y no se diligencia	Cálculo automático
DESCRIPCIÓN DE CONDICIÓN LEGITIMA DE LA EXCEPCIÓN	Implica la mención de una o varias de las excepciones taxativas que se establecen en los artículos 18 y 19 de la Ley 1712. Es decir, las contenidas en los literales de los artículos mencionados.	El campo es automático y no se diligencia	Cálculo automático
CALIFICACIÓN DEL ACTIVO DE ACUERDO A TRANSPARENCIA LEY 1712	**Información Pública.** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. **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 esta ley. **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 esta ley	El campo es automático y no se diligencia	Cálculo automático
Plazo de Clasificación o Reserva	El tiempo que dura la clasificación. En el caso de la información clasificada, el término es ilimitado, al tenor de lo establecido en el parágrafo único del artículo 18 de la Ley 1712. Para la información reservada, el tiempo máximo es de 15 años, de acuerdo con el artículo 22 del mismo cuerpo normativo, pero siempre bajo el entendido de que el lapso puede ser menor, según las circunstancias de cada caso.	El campo es automático y no se diligencia	Cálculo automático
CLASIFICACIÓN O RESERVA TOTAL O PARCIAL DE LA INFORMACIÓN	Permite establecer si existe clasificación o reserva sobre la información, y si dicha clasificación o reserva es sobre toda la información o parte de la información del activo **[Opciones disponibles]** *No Aplica* *Parcial* *Total*	Seleccione la clasificación o reserva que le aplica al activo de información de acuerdo con las opciones disponibles *Este campos solo se diligencia si la categoría seleccionada en el Tipo de Activo es "Datos / Información" o "Bases de datos".*	Líder de proceso / Colaborador designado

FECHA DE CALIFICACIÓN	Permite establecer la fecha desde la cual se determina que existe una clasificación o reserva sobre la información.	Registre en formato DD/MM/AAAA la fecha desde la cual se realiza la calificación o reserva. Si la fecha no es concreta o no se puede identificarla fácilmente puede: 1. Tome la fecha de registro o valoración del activo *Este campos solo se diligencia si la categoría seleccionada en el Tipo de Activo es "Datos / Información" o "Bases de datos".*	Líder de proceso / Colaborador designado
Frecuencia de actualización	Permite establecer la periodicidad o el segmento de tiempo en el que se actualiza la información, de acuerdo con su naturaleza y/o a la normatividad aplicable. **[Opciones disponibles]** *Diario* *Semanal* *Quincenal* *Mensual* *Bimensual* *Trimestral* *Cuatrimestral* *Semestral* *Anual* *Por demanda* *Otro* *No aplica*	Seleccione la periodicidad o el segmento de tiempo de acuerdo con las opciones disponibles *Este campos solo se diligencia si la categoría seleccionada en el Tipo de Activo es "Datos / Información" o "Bases de datos".*	Líder de proceso / Colaborador designado
Categoría lugares de consulta	Permite seleccionar el lugar o mecanismo principal donde se puede realizar la consulta de la información **[Opciones disponibles]** *Portales web propios* *Portales web de terceros* *Intranet* *Archivo fisico* *Archivos digitales* *Sistemas de información* *Bases de Datos*	Seleccione el lugar de consulta de la información de acuerdo con las opciones disponibles *Este campos solo se diligencia si la categoría seleccionada en el Tipo de Activo es "Datos / Información" o "Bases de datos".*	Líder de proceso / Colaborador designado
Detalle Lugar de Consulta	Permite registrar el lugar donde se ubica el activo de información donde puede ser consultado o se encuentra disponible	Registre el o los lugares donde se puede consultar la información o donde se encuentra disponible para consulta	Líder de proceso / Colaborador designado

DATOS ABIERTOS

CAMPO	DEFINICIÓN	INSTRUCTIVO	RESPONSABLE DE DILIGENCIAMIENTO
El activo se cataloga como dato abierto	Seleccionar **SÍ** o **NO**, si la información documentada conservada contiene datos abiertos, los cuales 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. La Ley establece la obligatoriedad de las entidades públicas de **"divulgar datos abiertos"**, teniendo en cuenta las excepciones de acceso a la información, asociadas a información clasificada y reservada establecidas en su título tercero, Artículos 18 y 19 de la Ley 1712 de 2014.	Seleccione si el activo se cataloga como información de datos abiertos.	Líder de proceso / Colaborador designado

REFERENCIAS

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Guía para la administración del riesgo. Bogotá. Diciembre 2014.

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES Guía para la administración del riesgo y diseño de controles en entidades públicas. Versión 5 Bogotá. 2020

ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN – ISO Norma Internacional ISO 31000. Ginebra, Suiza 2018

	MATRIZ PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	DIRECCIÓN TICS	
			FECHA: ENERO 2024

Nº	RIESGO	CAUSA DEL RIESGO	EFECTO DEL RIESGO	CONTROLES		DESCRIPCIÓN DEL CONTROL	SEVERIDAD		FRECUENCIA		DETECCIÓN		NIVEL DE CRITICIDAD	ACCIONES PREVENTIVAS O DE MEJORA
				SI	NO									
1	Indisponibilidad del sistema DGH.	Caída por fluido eléctrico, colección de la red, sistema operativo, virus, control de acceso no autorizado.	Inconveniencia de la atención, perdida de recursos, perdida de información.		X	Recurso humano disponible, ups, plan de contingencia, antivirus.	Menor	2	Frecuente	4	Alta	4	70	Trazadas en el plan de acción y la capacitación del sistema DGH.
2	Inconsistencia en la Información	Validación de la información.	Toma de decisiones erróneas.	X		Auditoría Médica, administrativa.	Mayor	4	Frecuente	4	Baja	7	50	Trazadas en el plan de acción y la capacitación del sistema DGH.
3	Sistematización de los procesos	Ausencia de un sistema integral	Débil integralidad entre los procesos.		X	Auditoría Médica, administrativa.	Mayor	4	Frecuente	4	Baja	7	30	Trazadas en el plan de acción y la capacitación del sistema DGH.
4	Inconveniencia a la solicitud de la capacitación de funcionarios sobre el sistema DGH	Disponibilidad de tiempo, disponibilidad de recursos.	Desactualización, ingreso o ausencia de información pertinente.	X		Evaluación del conocimiento.	Menor	2	Frecuente	4	Baja	7	70	Trazadas en el plan de acción y PETI y la capacitación del Sistema DGH.
5	Débil conocimiento de los funcionarios en el sistema DGH.	Plan de capacitación continua.	Débil integralidad de la información	X		Evaluación del conocimiento.	Menor	2	Ocasional	3	Baja	7	70	Trazadas en el plan de acción y PETI y la capacitación del Sistema DGH.
6	Debilidad en la aplicación y socialización de la seguridad de la información.	Aplicación de las políticas de seguridad de la información.	Uso inadecuado, perdida o fuga de la información.		x	Manual de políticas de seguridad de la información.	Mayor	4	Frecuente	4	Alta	4	50	Trazadas en el Plan Estratégico de tecnologías de la información PETI.
7	A causa de la no existencia de la política de seguridad aprobada por la gerencia, en consecuencia, no ha sido socializada, los funcionarios pueden incurrir en acciones que afecten la seguridad de la información.	No se encuentra implementada al 100% la política de la seguridad de la información en la E.S.E. UNA.	Uso inadecuado de la información, generación de quiebres que pueden atentar contra la información de la E.S.E UNA.		X	Se requiere aumentar el alcance de la seguridad de la información de la E.S.E UNA.	Mayor	4	Frecuente	4	Alta	4	70	Programada en el PETI
8	Debido a la falta unificación de criterios y la implementación de un protocolo que regule la entrega de la información contenidas en las bases de datos, se corre el riesgo de fuga y divulgación de la	Unificación de criterios y implementación de un protocolo, uso y procesamiento de la información de salida de las bases de datos de la E.S.E. UNA.	Fuga y divulgación de la información.		X	Se requiere planear, desarrollar e implementar el protocolo de uso de BD.	Mayor	4	Ocasional	3	Baja	7	50	Pendiente por desarrollar.

	información confidencial e interna.													
9.	A causa en las fallas presentadas al momento de crear, modificar o deshabilitar un usuario, por la notificación correcta y a tiempo por parte de Talento Humano y Asistencial.	Inconsistencia en la información por usuarios que ya no se encuentran en la institución o no cuentan con la autorización escrita.	Riesgo de perdida de información, acceso por personal que debería estar inhabilitados.		X	Se creo un formato de creación, modificación y eliminación de usuario.	Mayor	4	Frecuente	4	Alta	4	50	

CRITERIOS PARA LA EVALUACIÓN DEL RIESGO

PROBABILIDAD					
CASI SEGURO (5)					
FRECUENTE (4)					
OCASIONAL (3)					
RARO (2)					
REMOTA (1)					
	INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
	IMPACTO				