PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2024

Elaboro:	Reviso:	**Aprobó:**
Profesional Universitario Sistemas	Coordinador TIC	Comité de Gestión y Desempeño

TABLA DE CONTENIDO

1. INTRODUCCION

En los inicios de la seguridad, ésta se orientaba principalmente a la protección de propiedades físicas, almacenes, bodegas, productos, ya que era el mayor activo de las organizaciones. Sin embargo, hoy por hoy, la mayoría de actividades realizadas tanto a nivel empresarial como personal están envueltas en redes de datos administradas por sistemas de información computarizados que requieren un funcionamiento correcto garantizando su seguridad. En la actualidad, las organizaciones han tomado conciencia que el mayor activo de las mismas es la INFORMACIÓN, por ello, están tomando las precauciones necesarias para evitar fugas de datos o funcionamientos inadecuados en ellos.

Debido a la preocupación de contar con sistemas seguros, surge la Seguridad de la Información como medidas (estándares, normas, protocolos) tendientes a controlar e impedir el desarrollo de actividades no autorizadas sobre los activos de los sistemas de información (hardware – software – firmware – información), cumpliendo normas organizacionales o legales, que impidan el daño en los datos o acceso no autorizado, dejando al descubierto información confidencial, disminuyendo autenticidad o integridad u ocasionando lentitud en los procesos, el bloqueo a usuarios o equipos y/o disminución en el rendimiento en los mismos.

Múltiples factores influyen en un sistema de seguridad de la información, entre los que se mencionan: Apoyo del personal responsable de la dirección de la empresa, conocimiento del área de sistemas y colaboradores en general sobre tecnología, amenazas y riesgos, sentido de pertenencia de los usuarios, correcta administración de los equipos informáticos, establecimiento de políticas para limitar el acceso y establecer privilegios, soporte de los fabricantes de hardware y software, mapa de riesgos, políticas y procedimientos acordes a la realidad institucional.

De esta manera la seguridad de la información debe ser visualizada como un proceso más no como un bien o producto, de tal manera que aplicando las recomendaciones del estándar ISO 27001:2023, el cual es una norma internacional que describe cómo gestionar la seguridad de la información en una empresa, garantizamos tener un sistema de gestión de calidad óptimo disminuyendo riesgos detectados.

2. OBJETIVO

Diseñar e implementar mecanismos y estrategias que permitan asegurar la confidencialidad, integridad y disponibilidad de la información para soportar la adecuada gestión de los procesos de la ESE Hospital Universitario Erasmo Meoz y que se encuentran contempladas en el Modelo de Seguridad y Privacidad de la Información propuesto por el MINTIC.

2.1 OBJETIVOS ESPECIFICOS

- Cumplir con las leyes, regulaciones y obligaciones sectoriales aplicables a la Seguridad de la Información
- Identificar el inventario de los activos de información de una manera organizada para brindar una adecuada protección
- Establecer controles que mitiguen los riesgos a la infraestructura de seguridad de la información en la ESE HUEM
- Establecer lineamientos para la implementación de mejores prácticas de seguridad que oriente y obligue al uso adecuado de los recursos informáticos
- Definir mecanismos para la gestión de incidentes de seguridad de la información.
- Contar con planes de contingencia y continuidad que mantengan el nivel de servicio en unos límites predefinidos
- Mejorar la gestión de la seguridad de la información al interior de la entidad.

3. ALCANCE

Inicia con todos los datos o registros que se recolectan y a toda la información creada, procesada o utilizada, sin importar el medio, formato o presentación o lugar en el cual se encuentre hasta su divulgación o comunicación.

4. RESPONSABLE

Este programa debe ser liderado por la oficina de TIC y revisado por el Comité Institucional de Gestión y Desempeño

5. CAMPO DE APLICACIÓN

El Plan de Seguridad y Privacidad de la Información aplica a todos los funcionarios, colaboradores, terceros, procesos, servicios de la E.S.E. Hospital Universitario Erasmo Meoz y ciudadanía en general.

6. ACTUALIZACION

Debe ser revisado por lo menos cada dos (2) años, o antes si existiesen modificaciones que así lo requieran, para asegurar el mejoramiento continuo.

7. NORMATIVIDAD

Resolución 1995 de 1999. Por la cual se establece normas para el manejo de la historia clínica y se establecen la organización y manejo del archivo de historias clínicas, custodia, acceso y seguridad[1]. La entidad como prestadora de servicios de salud, tiene bajo su custodia la información de historia clínica de los pacientes, siendo esta norma de obligatorio cumplimiento para el hospital ya que indica los registros que debe contener, quienes pueden tener acceso a ella, la custodia, la seguridad y condiciones de almacenamiento.

Ley 1266 de 2008. Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Tiene por objeto desarrollar el derecho constitucional de conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, además de los derechos, libertades y garantías relacionadas con la recolección, tratamiento y circulación de datos personales, así como el derecho a la información[2]. La entidad como Operador de información, por recibir información de datos personales directamente del titular, tiene la administración de los mismos, por tanto, está obligado a garantizar la protección de estos datos.

Ley 1341 de 2009. 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 de Espectro y se dictan otras disposiciones. Reglamentada por el decreto 2693 de 2012 y 2573 de 2014[3]. A través de esta ley se facilita el libre acceso y sin discriminación a los habitantes del territorio nacional a la Sociedad de la información y establece el régimen de protección al usuario entre otras cosas.

Ley 1273 de 2009. Por el cual se modifica el código Penal, creando u nuevo bien jurídico tutelado llamado 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[4]. En esta norma, tipifica y protege la información de los datos,

[1]Resolución 1995 de 199. Recuperado de https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf
[2]Ley 1266 de 2008. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488
[3]Ley 1431 de 2009. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913
[4]Ley 1273 de 2009. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

sentando en el código penal algunos delitos informáticos con sus respectivas penas. A nivel general tenemos:

- Suplantación de sitios web para capturar datos personales.
- Violación de datos personales.
- Uso de software malicioso.
- Daño informático.
- Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Acceso abusivo a un sistema informático.

Cuya pena en prisión puede ir de 48 a 96 meses y multa de 100 a mil salarios mínimos mensuales legales vigentes.

- Interceptación de datos informáticos.

Incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- Transferencia no consentida de activos.

Incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes

- Hurto por medios informáticos y semejantes

Se aplicará las penas establecidas en el art.240 del código Penal. La pena será de 5 a 12 años de prisión.

También define aquellos agravantes que aumentarán las penas dispuestas, como por ejemplo: aquellos cometidos sobre redes oficiales o del sector financiero, por servidor público en ejercicio de sus funciones, aprovechando la confianza depositada por el poseedor de la información, publicando información en perjuicio de otro, obteniendo provecho para sí mismo o para un tercero, con fines terroristas, generando riesgo para la seguridad nacional, si quien cometiere estos delitos es el responsable de la administración, manejo o control, se le impondrá pena de inhabilitación hasta por tres años para el ejercicio de su profesión relacionada con los sistemas de información.

Ley estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales, cuyo objeto es desarrollar el derecho constitucional a conocer, actualizar y rectificar informaciones que se hayan recogido en bases de datos o archivos, así como el derecho a la información consagrado[5]. Sobre el tratamiento de datos personales se aplican diferentes principios, entre ellos, el de transparencia, acceso y circulación restringida, de seguridad y confidencialidad.

[5]Ley estatutaria 1581 de 2012. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Resolución 3100 de 2019. Por la cual se define los estándares de habilitación para las instituciones prestadoras de servicios de salud, dentro de ellos Historia Clínica y Registros, que busca la existencia y cumplimiento de procesos que garanticen la historia clínica por paciente y las condiciones técnicas de su manejo y el de los registros de procesos clínicos que se relacionan directamente con los principales riesgos propios de la prestación de servicios, estableciendo que para la gestión de las historias en medios electrónicos, se debe garantizar la confidencialidad y seguridad, sin que se puedan modificar los datos una vez se guarden los registros, garantizando la confidencialidad del documento protegido legalmente por reserva .[6]

Decreto 903 de 2014. Por el cual se dictan disposiciones en relación con el Sistema Único de Acreditación en salud. Dicta disposiciones y realiza ajustes al sistema único de acreditación en Salud, como componente del Sistema Obligatorio de Garantía de Calidad de la Atención de salud. [7] El sistema de acreditación es voluntario, y las entidades que deciden implementarlo, deben comprobar el cumplimiento de niveles de calidad superiores a los requisitos mínimos obligatorios (habilitación).

Manual de Acreditación en salud. El Ministerio de Salud y Protección Social adoptará los manuales, los cuales serán de uso libre, podrán ser ajustados periódicamente y de manera progresiva. El Manual de Acreditación está dividido en Grupos de estándares que a su vez contienen criterio y estándares, así como el estándar de mejoramiento por cada grupo. Los estándares que aplican para la institución son estándares del proceso de atención al cliente asistencial, estándares de direccionamiento, estándares de gerencia, estándares de gerencia del talento humano, estándares de gerencia del ambiente físico, estándares de gestión de tecnología, estándares de gerencia de la información, estándares de mejoramiento de la calidad.

Para el presente proyecto aplicado, se realiza especial énfasis en el Grupo de estándares de Gerencia de la Información, el cual busca la integración de las áreas asistenciales y administrativas en relación con la información clínica y administrativa buscando que los procesos tengan información adecuada para la toma de decisiones y obliga a la implementación de mecanismos y estrategias para garantizar la seguridad y confidencialidad de la información, desarrollando un plan de gerencia de la información, con fundamento en el ciclo de mejoramiento continuo.[8]

La organización debe cumplir con criterios como el estándar 144. Existen mecanismos estandarizados, implementados y evaluados para garantizar la seguridad y confidencialidad de la información, cuyos criterios son: la seguridad y confidencialidad;

[6] Resolución 3100 de 2019.
[7] Decreto 903 de 2014. Recuperado de http://www.acreditacionensalud.org.co/userfiles/file/2015/Decreto%200903%20de%202014.pdf
[8] Manual de Acreditación en salud. Recuperado de http://www.acreditacionensalud.org.co/Documents/Manual%20AcreditSalud%20AmbulyHosp2012.pdf

acceso no autorizado; pérdida de información; manipulación; mal uso de los equipos y de la información, para fines distintos a los legalmente contemplados por la organización; deterioro, de todo tipo, de los archivos; los registros médicos no pueden dejarse o archivarse en sitios físicos donde no esté restringido el acceso a visitantes o personal no autorizado; existe un procedimiento para la asignación de claves de acceso; existencia de backups y copias redundantes de información; control documental y de registros; indicadores de seguridad de la información.

Decreto 2573 de 2014. Por el cual se establecen los lineamientos generales (lineamientos, instrumentos y plazos) de la Estrategia de Gobierno en línea, para garantizar el aprovechamiento de las Tecnologías de la Información y Comunicaciones y se reglamenta parcialmente la Ley 1341 de 2009[9].

Ley 1712 de 2014. 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. Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.[10]

Resolución 3564 de 2015. Tiene por objeto establecer los lineamientos respecto de los estándares para publicación y divulgación de la información, accesibilidad en medios electrónicos para población en situación de discapacidad, formulario electrónico para la recepción de solicitudes de acceso a información pública, condiciones técnicas para la publicación de datos abiertos y condiciones de seguridad de los medios electrónicos, que se establecen en los artículos 2.1.1.2.1.1, 2.1.1.2.1.11, y el parágrafo 2 del artículo 2.1.1.3.1.1 del Decreto N° 1081 de 2015. [11]

CONPES 3854 de 2016. Política Nacional de Seguridad digital, el cual adopta la gestión del riesgo como núcleo central para la implementación de seguridad digital de manera proactiva.

ISO 27001:2023 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.

[9] Decreto 2573 de 2014. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60596#14
[10] Ley 1712 de 2014. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882
[11] Res.3564 de 2015. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=66249

8. DEFINICIONES

ACTIVOS DE LA INFORMACIÓN: Elementos de valor que representa la información en la empresa como son, datos, software, hardware, elementos de redes y comunicaciones, infraestructura y recursos humanos. Tiene valor para los procesos institucionales, independientemente de su ubicación, puede ser un documento físico, un archivo guardado en un equipo, un aplicativo o cualquier elemento que permita almacenar información útil para el hospital.

AMENAZAS: Cualquier situación que se puede presentar en la entidad dañando un activo de información, mediante la explotación de una vulnerabilidad.

ANÁLISIS DE RIESGOS: Es un elemento fundamental dentro del proceso de implantación de un SGSI debido a que es en esta fase donde se cuantifica la importancia de los activos para la seguridad de la organización.

CONFIDENCIALIDAD: Capacidad de no divulgar o publicar información sensible de una empresa a personas no autorizadas. Como ejemplo tenemos los accesos no autorizados, fugas y filtraciones de información. Al tener fallo en esa característica de la información, supone el incumplimiento de leyes y compromisos en relación a la custodia de datos, además que la organización evidenciaría que no es competente para el manejo de datos.

CONTROL. Toda actividad o procesos encaminados a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizaciones, buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

DISPONIBILIDAD: Consiste en tener los activos disponibles cuando se requiere su uso. La falta de este atributo evidencia una interrupción del servicio y afecta la productividad de la organización.

EVENTO DE SEGURIDAD INFORMÁTICA: Un evento de seguridad informática es una ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de medidas de seguridad (safeguards), o una situación previamente desconocida que pueda ser relevante para la seguridad. [ISO 18044]
Por ejemplo: un usuario se conecta a un sistema, un intento fallido de un usuario para ingresar a una aplicación, el firewall que permite o bloquea un acceso, una notificación de un cambio de contraseña de un usuario privilegiado, etc. Un Evento de Seguridad Informática no es necesariamente una ocurrencia maliciosa o adversa.

IMPACTO: Es el alcance del daño que se produce en un activo cuando sucede una amenaza.

INCIDENTE DE SEGURIDAD: Un incidente de seguridad informática es la violación o amenaza inminente a la violación de una política de seguridad de la información implícita o explícita. También es un incidente de seguridad un evento que compromete la seguridad de un sistema (confidencialidad, integridad y disponibilidad). Un incidente puede ser denunciado por los involucrados, o indicado por un único o una serie de eventos de seguridad informática. [NIST800-61, ISO 18044].
Como ejemplos de incidentes de seguridad podemos enumerar:

- Acceso no autorizado
- Robo de contraseñas
- Robo de información
- Denegación de servicio

INTEGRIDAD: Característica de mantener la información de manera intacta sin tener modificaciones. Al fallar este elemento afecta directamente el correcto funcionamiento de la organización.

INFORMACIÓN: Datos que maneja la empresa ya sea en forma digital o impresa.

RIESGO: Aquella eventualidad que imposibilita el cumplimiento de un objetivo.

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

SGSI. Sistema de Gestión de Seguridad de la Información. El desarrollo de un Sistema de gestión de seguridad de la información es un proceso sistemático, documentado que se realiza para garantizar que la seguridad de la información es gestionada correctamente, buscando mantener la confidencialidad, integridad y disponibilidad para contrarrestar los riesgos a los cuales puede estar expuesta la entidad, lo cual es precisamente el objeto de aplicar la seguridad de la información y la seguridad informática.

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

VULNERABILIDAD: Es toda debilidad del sistema informático que puede ser utilizada para causar un daño. Corresponde a las ausencias o fallas en los controles para proteger un activo.

9. CONTENIDO GENERAL

La seguridad de la información incluye tres dimensiones principales: la confidencialidad, la disponibilidad y la integridad. Con el objetivo de garantizar el procesamiento sostenido así como su continuidad, y minimizar impactos, la seguridad de la información conlleva la aplicación y la gestión de medidas de seguridad adecuadas que implican la consideración de una amplia gama de amenazas.

La seguridad de la información se consigue mediante la implementación de un conjunto de controles aplicables, seleccionados a través del proceso de gestión de riesgo que se haya elegido y gestionado por medio de un SGSI, empleando políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información identificados.

Estos controles necesitan ser especificados, implementados, monitoreados, revisados y mejorados cuando sea necesario, para garantizar que la seguridad y el cumplimiento de la normatividad se cumplan. Estos controles de seguridad de la información deben integrarse de forma coherente con los procesos de la institución.

Un gran número de factores son fundamentales para la implementación exitosa de un SGSI que permita a la organización cumplir con sus objetivos. Entre ellos tenemos:

a) Que la política, los objetivos y actividades de seguridad de la información estén alineadas con los objetivos institucionales.

   La Gerencia de la entidad, establece una Política de Seguridad de la Información, en la que se incluyen los objetivos de seguridad de la información (Confidencialidad, Integridad, Disponibilidad) e incluye el compromiso de implementar mecanismos y estrategias para soportar la adecuada gestión de los procesos de la organización, así como el de mejora continua del Sistema de Gestión de Seguridad de la Información.

   Esta resolución se encuentra documentada, comunicada y disponible para su consulta.

b) Un enfoque y un marco para el diseño, ejecución, seguimiento, mantenimiento y mejora de la seguridad de la información en consonancia de la cultura de la organización, consignado en este Programa de Seguridad de la Información.

c) El apoyo visible y el compromiso de todos los niveles de la Dirección, especialmente de alta Dirección; evidenciado en la asignación de roles y responsabilidades de la Resolución Interna.

d) La revisión continúa de la normatividad y aplicabilidad para el cumplimiento de requisitos de la seguridad de la información que deben estar consignadas en el Normograma institucional.

e) Obtener un inventario de activos de información con las siguientes actividades: Definición, Revisión, Actualización y Publicación, las cuales se reflejan documentalmente en la Matriz de Inventario y Clasificación de Activos de Información.

f) EL conocimiento y entendimiento de los requisitos de protección de los activos de información obtenido mediante la aplicación de la gestión del riesgo de la seguridad de la información.

La gestión del riesgo de seguridad de la información se realiza valorando las posibles consecuencias que resultarían si los riesgos identificados con la pérdida de confidencialidad, integridad y disponibilidad de los activos de la información llegase a materializarse, valorando de forma realista la probabilidad de ocurrencia y determinando los niveles de riesgo.

El Hospital Universitario Erasmo Meoz adopta la metodología propuesta en la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas como documento orientador para la implementación de la gestión de riesgos de seguridad digital que, entre otros aspectos, pretende incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en cada entidad pública.

Una vez evaluados los riesgos de seguridad de la información se compara los resultados del análisis de riesgos con los criterios de riesgo establecidos, priorizando los riesgos analizados para de esta manera formular un plan de tratamiento de riesgos de seguridad de la información; obteniendo la aprobación del plan y la aceptación de los riesgos residuales de seguridad de la información por parte de los dueños de los riesgos.

g) Generar un documento que oriente a los usuarios en el uso adecuado de los activos de la información, presentando en forma clara y coherente las directrices a seguir para el cumplimiento de los requisitos de Confidencialidad, Integridad y Disponibilidad de la información consignados en la política de seguridad. Este documento lo deben conocer, acatar y cumplir todos los miembros de la entidad, bajo el liderazgo del área de TIC’s.

h) Un plan efectivo de concienciación, formación y educación sobre seguridad de la información, informando a todos los empleados y otras partes pertinentes de sus obligaciones en seguridad de la información establecidas en las políticas de seguridad de la información, normas, etc., y motivarlos a actuar en consecuencia.

Las personas que trabajan bajo el control de la organización deben ser conscientes de los beneficios de una mejora del desempeño en seguridad de la información; y las implicaciones de no cumplir con los requisitos del sistema de gestión de la seguridad de la información. De igual manera, se debe establecer los medios que se usen para contribuir a la divulgación de la información y se debe consignar en el Plan de Capacitación institucional.

i) Un proceso eficaz de gestión de incidentes de seguridad de la información; que oriente a un plan de respuesta que ayuda a evaluar la naturaleza del caso, identificar posibles implicaciones del caso si éste aumenta (o disminuye) en gravedad, establece líneas de comunicación con respecto al mismo, ayuda a montar y poner en marcha el o los equipo(s) de respuesta capacitado(s) para manejar el evento y fungir como un punto de decisión para el lanzamiento de otros planes como de recuperación de desastres, de continuidad de negocio, entre otros.

j) Un enfoque efectivo de gestión de la continuidad y plan de contingencia; que busca contar con medidas para una pronta recuperación ante los desastres, minimizando el trauma en la prestación del servicio y reanudar lo antes posible las operaciones habituales en el manejo del registro de datos y procesamiento de información; estableciendo un periodo de recuperación mínimo, recuperación de la situación inicial anterior al incidente de seguridad, analizando los resultados y los motivos del incidente, y disminuyendo el trauma ocasionado en el cese de las actividades de la ESE.

k) Un sistema de medición utilizada para evaluar el desempeño en la gestión de la seguridad de la información y para proporcionar sugerencias de mejora. La ESE HUEM debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información, evaluando periódicamente (mínimo cada año) con herramientas la línea base de seguridad de la información para establecer el avance y las metas a cumplir para seguir con el proceso de mejora continua.

10. CRONOGRAMA

Actividad	Responsable	I TRIM	II TRIM	III TRIM	IV TRIM
Realizar autodiagnóstico del Estado actual de seguridad de la información y establecer el nivel de madurez del mismo	Profesional Universitario Sistemas	X			
Diseñar plan de trabajo y estrategias conforme al autodiagnóstico generado	Profesional Universitario Sistemas/ Coordinador TICS		x		
Revisar la actual política de seguridad de la información e incorporar los aspectos pendientes	TIC				X
Actualizar Plan de continuidad y contingencia informática en la ESE HUEM	TIC				X
Fortalecer conocimientos de seguridad de la información a los colaboradores en la entidad	TIC	X	X	X	X
Cumplimiento del Plan de tratamiento de riesgos de seguridad y privacidad de la información	TIC	X	X	X	X

11. INDICADORES

INDICADOR	FORMULA DE CALCULO	FUENTE	META	FRECUENCIA	RESPONSABLE
EFECTIVIDAD DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN - ISO 27001:2023 ANEXO A	Sumatoria de la calificación de Evaluación de Efectividad de controles / Total de dominios evaluados	Instrumento de identificación de la línea base de seguridad del MINTIC	65	Anual	Profesional Universitario Sistemas

12. CONTROL DE CAMBIOS

VERSIÓN	FECHA	PAGINA	APROBÓ	DESCRIPCIÓN DE CAMBIOS
1	30 de Noviembre	1-14	Comité de Gestión y Desempeño	Creación del Documento por cambio normativo
2	27 de Enero de 2021	1-14	Comité de Gestión y Desempeño	Se actualiza por mejoramiento continuo vigencia 2022
3	26 de Enero de 2023	1-15	Comité de Gestión y desempeño	Se actualiza por mejoramiento continuo vigencia 2023
4	25 de Enero de 2024	1-15	Comité de Gestión y desempeño	Actualización Vigencia 2024 cambio norma técnica ISO 27001:2023