Empresa Social del Estado
HOSPITAL MENTAL DE ANTIOQUIA
María Upegui
HOMO

GOBERNACIÓN DE ANTIOQUIA
República de Colombia

Empresa Social del Estado
HOSPITAL MENTAL DE ANTIOQUIA
María Upegui
HOMO

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

2023

UNIDOS

Calle 38 No 55-310 Bello-Colombia - Teléfono: (4) 4448330 Fax: (4) 4527479Línea de atención 018000 417474 – Nit: 890-905-166-8-www.homo.gov.co

1. JUSTIFICACION

En el ESE HOMO, uno de los más importantes activos es la información, que diariamente captamos en la prestación de nuestros servicios. Teniendo en cuenta lo anterior y conscientes de su importancia, podemos indicar que se deben adoptar medidas de seguridad para la información, para las posibles contingencias que pueden afectar dicho activo.

La estrategia de respaldo y continuación del negocio respondiendo a eventos imprevistos o críticos hacen desviar del método de trabajo original, constituyéndose en el plan para determinar cómo actuar rápidamente y encaminar los sistemas de información de la E.SE. HOMO.

2. OBJETIVO

Detallar el plan de tratamiento de riesgos, de tal forma que se definen y aplican los controles con los cuales se buscan mitigar la materialización de los riesgos de seguridad de la información en la E.S.E Hospital Mental de Antioquia. De esta forma se busca que, mediante el tratamiento de los riesgos y la mejora continua de la Seguridad y Privacidad de la Información, las partes interesadastengan mayor confianza en el tratamiento de la información que se almacena y maneja en la Entidad, y de esta manera reducir los impactos negativos que puedan generar en la gestión institucional.

Objetivos específicos

- Mejorar continuamente los conocimientos del equipo de trabajo en materia de seguridad digital y prevención de riesgos.
- Preparar a todos los colaboradores para responder ante incidentes de seguridad que afecten los activos de información.
- Mejorar la confianza de los grupos de valor en nuestra capacidad institucional para preservar la seguridad de la información.

3. ALCANCE

El tratamiento de los riesgos de seguridad de la información es de estricta aplicabilidad y cumplimiento por parte de todos los funcionarios, contratistas que presten sus servicios o tengan algún tipo de relación con la Entidad; dicho tratamiento de riesgo debe involucrar a todos los procesos y actividades desarrolladas por la Entidad, en especial aquellos que impactan directamente la consecución de los objetivos misionales.

4. MARCO LEGAL

Norma	Detalle
Constitución Política de Colombia 1991	Artículo 15, reconoce como derecho fundamental el Habeas Data y articulo 20, Libertad de información.
Decreto 612 de 4 de abril de 2018	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 14 de junio de 2018	por el cual se establecen los lineamientos generales de la política de Gobierno digital
Guía 7 gestiones de riesgos. Modelo de Seguridad y Privacidad de la Información.	Modelo de Seguridad y Privacidad de la Información. Ministerio de las Tecnologías y la información y las comunicaciones, estrategia de Gobierno Digital.
Guía 8 controles de seguridad y privacidad de la información.	Modelo de seguridad y privacidad de la información. Ministerio de las Tecnologías y la información y las comunicaciones, estrategia de Gobierno Digital.

5. DEFINICIONES

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Análisis de Riesgo: Uso sistemático de la información para identificar fuentes y estimar el riesgo (Guía ISO/IEC 73:2002).

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar su importancia.

Factor de riesgo: Agente ya sea humano o tecnológico que genera el riesgo

Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: propiedad de exactitud y completitud.

Mapa de riesgos: documento con la información resultante de la gestión del riesgo.

Nivel de riesgo: Da el resultado en donde se ubica el riesgo por cada activo de información.

Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

Riesgo: Efecto de la incertidumbre sobre el cumplimiento de los objetivos.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Tratamiento del riesgo: Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

Riesgo: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o elcumplimiento de los objetivos institucionales.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera.

También se pueden generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Riesgo positivo: Posibilidad de ocurrencia de un evento o situación quepermita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

Seguridad de la información: Este principio busca crear condiciones de uso confiables 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.

6. RECURSOS HUMANOS FINANCIEROS

La administración y operación de los sistemas para la seguridad de la información de nuestro sistema actual debe ser siempre una de las prioridades en cada uno de los centros hospitalarios, clínicas y todo tipo de instituciones públicas o privadas que presten servicio de salud.
Esta es una operación que debe ser ejecutada por personal capacitado y con las competencias necesarias para la manipulación de estos equipos, por lo general, técnicos, tecnólogos o ingenieros del área para que estos planes de seguridad y privacidad de la información sean operativos y seguros con las herramientas que tenemos actualmente. Sin embargo, cabe aclarar que en este campo la experiencia también es un factor determinante que juega a favor de aquellos que llevan más tiempo desempeñando esta labor, y en algunos casos, esta misma experiencia les ha permitido desarrollar ajustes o avances para el mejoramiento del funcionamiento de estas herramientas de seguridad y privacidad de la información.

Por lo tanto, como recurso humano para el desarrollo de este Plan se Requiere:

1. (1) Un ingeniero de telecomunicaciones directamente contratado por el hospital, que pueda gestionar toda la parte administrativa que conlleva el subproceso y al mismo tiempo que pueda sustentar las auditorias que se presenten, además del soporte y apoyo al área de telemedicina y otros servicios que estén relacionados con estos servicios en representación directa de la E.S.E HOSPITAL MENTAL DE ANTIOQUIA MARIA UPEGUI HOMO.

2. (1) Un ingeniero de sistemas o afines directamente contratado por el hospital o contratista por prestación de servicios, que pueda gestionar toda la parte administrativa que conlleva el subproceso y al mismo tiempo que pueda sustentar las auditorias que se presenten, además del soporte o apoyo al área de tecnología en centro de datos, servidores, equipos de cómputo, otros dispositivos y servicios que necesita este área para suoperación en representación directa de la E.S.E HOSPITAL MENTAL DE ANTIOQUIA MARIA UPEGUI HOMO.

3. (1) Un técnico, tecnólogo o ingeniero de sistemas o afines directamente contratado por el hospital o contratista por prestación de

servicios, que pueda gestionar el sistema de información actual que tiene la empresa con la versión SXG5 Advacend de la empresa XENCO sobre motor de bases de datos ORACLE aplicación cliente servidor y otras funciones de apoyo al área de sistemas que necesita este área para su operación en representación directa de la E.S.E HOSPITAL MENTAL DE ANTIOQUIA MARIA UPEGUI HOMO.

4. (2) Dos técnicos o tecnólogos directamente contratados por el hospital , contratistas de prestación de servicios o por cooperativa, para el servicio de mantenimiento y soporte a la infraestructura de sistemas y comunicaciones, para todas las actividades técnico operativas y apoyo a la gestión correspondiente a la ejecución de los mantenimientos predictivos, preventivos y correctivos programados y no programados que se puedan presentar con los sistemas de información actual más el soporte a los usuarios finales en representación directa de la E.S.E HOSPITAL MENTAL DE ANTIOQUIA MARIA UPEGUI HOMO.

5. (1) Un contratista técnico, tecnólogo en mantenimiento, para todas las actividades técnico operativas y apoyo a la gestión correspondientes la ejecución de los mantenimientos predictivos, preventivos y correctivos programados y no programados que se puedan presentar con la infraestructura de datos, comunicaciones, potencia, regulada, sistema de seguridad de cámaras y otros dispositivos para los sistemas de información en representación directa de la E.S.E HOSPITAL MENTAL DE ANTIOQUIA MARIA UPEGUI HOMO.

7. PRESUPUESTO

PLAZO CONTRACTUAL
El plazo contractual se estima en doce (12) meses, contados a partir del primero (01) de enero de 2022 hasta el Treinta y uno (31) de diciembre de 2023, previo el cumplimiento de las obligaciones de expedición de pólizas o garantías a que haya lugar.
LUGAR DE EJECUCIÓN

El objeto de lo contratado se prestará en las instalaciones de la ESE Hospital Mental de Antioquia del municipio de Bello, calle 38 No. 55-310. Y donde por necesidades del servicio el Hospital necesite prestar algún servicio extramural, siempre y cuando sea afín a su Misión.

VALOR ESTIMADO Y JUSTIFICACIÓN	
Rubro y disponibilidad presupuestal; con un valor de **MIL CUARENTA Y CUATRO MILLONES DOSCIENTOS CUARENTA Y CUATRO PESOS / ML** ($1.044.000.244)	Rubro: Servicios de tecnología de la información (TI) de consultoría y de apoyo Según certificado de Disponibilidad Presupuestal expedido por la técnica administrativa

El presente presupuesto ha sido estimado de acuerdo con:

DETALLE	VALOR
Nómina de 6 personas (Personal de departamento TI proyectado y actual.	$317.182.000 (Aprox.)
TOTAL:	**$317.182.000**

MODALIDAD DE SELECCIÓN		
El proceso de selección que debe ser utilizado para suplir las necesidades que le asisten a esta entidad hospitalaria y contenidas en el presente estudio previo es:		
Contratación Directa o Privada	Contratación con una sola oferta	**X**
	Contratación con tres ofertas	
Convocatoria Pública		

8. METODOLOGIA

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

En el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información –SGSI de la E.S.E Hospital Mental de Antioquia, se busca prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad de la información, por lo cual es importante controlar y establecer los riesgos de seguridad de la información.

De esta forma, se garantiza el tratamiento de los riesgos de seguridad de la información y la gestión de riesgo positivo u oportunidad.

RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

A continuación, se visualizan los riesgos de Seguridad de la Información, los cuales se encuentran asociados al Sistema de Gestión de Seguridad de la Información-SGSI de la E.S.E Hospital Mental de Antioquia.

1. Revelar información sensible o confidencial para beneficio propio o de un tercero.
2. Destrucción de información con fines ilícitos.
3. Fuga de información y detrimento al patrimonio y /o Deterioro de la reputación de la ESE HOMO.
4. Pérdida de confidencialidad, integridad o disponibilidad de información sensible de la Entidad.
5. Ataques contra el sistema (negación del servicio, manipulación de software, manipulación de equipo informático entre otros).

R1- Revelar información sensible o confidencial para beneficio propio o de un tercero.	
Nombre del plan de tratamiento	Adopción de un esquema de clasificación de la información
Proceso:	Todos los procesos de la Entidad
Descripción del plan	La no disposición de un plan definido de clasificación de la información se configura como alto riesgo. Adoptar el manejo especial para la información asegurando los niveles de seguridad en todos sus niveles, los propietarios de los activos de información son

	responsables de ellos. Se debe realizar la socialización al interior de la organización de las recomendaciones de MINTIC en la "Guía para la Gestión y Clasificación de Activos de Información". Esta contiene los criterios de clasificación de la información.		
Riesgos asociados	Fuga de información Divulgación no permitida de información Detrimento patrimonial Pérdida de la disponibilidad		
Controles asociados	A.9.1.1.2 Gestión de derechos de acceso privilegiado. A.11 Seguridad física y del entorno. A.17.1.1 Planificación de la continuidad de la seguridad de la información.		
Metodología	ISO 27001		
Actividades del plan	1. Divulgar y gestionar el cumplimiento de la política de seguridad digital.	Responsable: Profesional Universitario - Sistemas	Periodicidad: 30 junio 2023 30 noviembre 2023
	2. Construir la Matriz de Clasificación y Registro de Activos de Información	Responsable: Profesional universitario – Técnica Gestión documental	Periodicidad: 30 noviembre de 2023
	3. Verificar la adecuada definición e	Responsable: Profesional Universitario -	Periodicidad: 30 junio 2023

	implementación de los esquemas de perfiles de acceso a la información definidos.	Sistemas	
Recursos requeridos	Personas: funcionarios y Contratistas designados por profesional universitario de Sistemas de información de la ESE HOMO. Tecnológicos: Pc´s y Servidores		
Responsable del Plan	Profesional universitario - Sistemas		

R2- Destrucción de información con fines ilícitos.	
Nombre del plan de tratamiento	Plan de Control de acceso, de la seguridad físico y del entorno
Proceso:	Todos los procesos de la Entidad.
Descripción del Plan de Tratamiento:	La no definición de las condiciones de acceso tanto físico al centro de datos como lógico a las bases y repositorios de datos genera alto riesgo. Es necesario la adopción de un protocolo de acceso al centro de datos de la entidad, así como asegurar los controles de acceso a la información lógica de acuerdo con los perfiles que se definan.
Riesgos Asociados	Perdida de la Disponibilidad Perdida de la Integridad Riesgo reputacional
Controles asociados	A.9 Control de Acceso. A.11 Seguridad física y del entorno. A.12 Seguridad de las Operaciones. A.17.1.1 Planificación de la continuidad de la seguridad de la información

Metodología	ISO 27001		
Actividades del plan	1. Generar y divulgar un Protocolo de acceso al centro de datos de la entidad	Responsable: Profesional universitario - Sistemas	Periodicidad: 30 marzo 2023
	2. Verificar la adecuada definición e implementación de los esquemas de perfiles de acceso a la información definidos.	Responsable: Profesional Universitario – Sistemas	Periodicidad: 30 junio 2023
	3. Validar la correcta y adecuada toma de copias de respaldo	Responsable: Profesional Universitario – Sistemas	Periodicidad: 30 abril de 2023 30 julio de 2022 30 noviembre 2023
Recursos requeridos	Personas: funcionarios y Contratistas designados por profesional universitario de Sistemas de información de la ESE HOMO. Tecnológicos: Pc´s y Servidores		
Responsable del Plan	Profesional universitario - Sistemas		

R3 - Fuga de información			
Nombre del plan de tratamiento	Plan de aseguramiento de la Información.		
Proceso:	Todos los procesos de la Entidad.		
Descripción del Plan de Tratamiento:	La no adopción de un esquema claro de aseguramiento de la información, y controles de acceso, genera alto riesgo. Al adoptar uno adecuado se está asegurando que la información reciba los niveles de protección y acceso adecuados a fin de no permitir perdida de información.		
Riesgos Asociados	Detrimento al patrimonio y /o Deterioro de la reputación Perdida de Disponibilidad Perdida de la Confidencialidad		
Controles asociados	A.9 Control de Acceso A.11 Seguridad física y del entorno A.17.1.1 Planificación de la continuidad de la seguridad de la información		
Metodología	ISO 27001		
Actividades del plan	1. Verificar la adecuada definición e implementación de los esquemas de perfiles de acceso a la información definidos.	Responsable: Profesional Universitario – Sistemas	Periodicidad: 30 junio 2023
	2. Validar la correcta y adecuada	Responsable: Profesional Universitario –	Periodicidad: 30 abril de 2023 30 julio de 2023

	toma de copias de respaldo	Sistemas	30 noviembre 2023
Recursos requeridos	Personas: funcionarios y Contratistas designados por profesional universitario de Sistemas de información dela ESE HOMO. Tecnológicos: Pc´s y Servidores		
Responsable del plan	Profesional universitario - Sistemas		

R4 – Ataque cibernético sobre la plataforma tecnológica	
Nombre del plan de tratamiento	Plan de continuidad del negocio
Proceso:	Todos los procesos de la Entidad.
Descripción del Plan de Tratamiento:	Las amenazas cada vez se tornan en diferentes escenarios como es el terrorismo, paros a nivel nacional, la globalización y las ciber-amenazas que han mostrado la necesidad de incorporar nuevas estrategias con el fin de garantizar la continuidad de las operaciones ante un evento cada vez más dinámico en la relacionado con el tipo de riesgos al que se está expuesto. Este plan apunta a las estrategias dispuestas para el restablecimiento y recuperación parcial o total de las operaciones después de una interrupción no planeada o un desastre.
Riegos asociados	A.9.Control de Acceso A.11 Seguridad física y del entorno A.12 Seguridad de las Operaciones A.16 gestión de incidentes de Seguridad de la Información A.17.1.1 Planificación de la continuidad de la seguridad de la información

Metodología	ISO 27001		
Actividades del plan	1. Revisión periódica de controles para evitar pérdida de información.	Responsable: Profesional Universitario – Sistemas	Periodicidad: 30 abril de 2023 30 julio de 2023 30 noviembre 2023
	2. Validar la correcta y adecuada toma de copias de respaldo.	Responsable: Profesional Universitario – Sistemas	Periodicidad: 30 abril de 2023 30 julio de 2023 30 noviembre 2023
	3. Mantener actualizado y vigente el esquema de seguridad perimetral definido.	Responsable: Profesional Universitario – Sistemas	Periodicidad: 30 junio 2023 30 noviembre 2023
	4. Mantener actualizado y vigente el esquema de antivirus definido.	Responsable: Profesional Universitario – Sistemas	Periodicidad: 30 julio de 2023
Recursos requeridos	Personas: funcionarios y Contratistas designados por profesional universitario de Sistemas de información de la ESE HOMO. Tecnológicos: Pc´s y Servidores		

Responsable del plan	Profesional universitario - Sistemas

R5 - Inadecuado tratamiento de datos personales			
Nombre del plan de tratamiento			
Proceso:	Todos los procesos de la Entidad.		
Descripción del Plan de Tratamiento:	Uso no adecuado de los datos sensibles de los usuarios, lo que repercute en una violación de los derechos constitucionales.		
Riegos asociados	Detrimento al patrimonio y /o Deterioro de la reputación Perdida de confidencialidad.		
Controles asociados	A.9.Control de Acceso A.17.1.1 Planificación de la continuidad de la seguridad de la información		
Metodología	ISO 27001		
Actividades del plan	Validar que se cuente con definiciones y políticas de seguridad digital que aseguren la privacidad y la protección de los datos personales, de acuerdo con los lineamientos internos para la calificación de la	Responsable: Profesional Universitario – Sistemas	Periodicidad: 30 noviembre de 2023

	información y las disposiciones generales que exige la legislación nacional.		
Recursos requeridos	Personas: funcionarios y Contratistas designados por profesional universitario de Sistemas de información de la ESE HOMO.		
Responsable del plan	Profesional universitario - Sistemas		

La Política de autorización y protección de bases de datos personales de la ESE HOMO, está alineada con el modelo institucional y es una de las fuentes de mejora, Para el tratamiento, especialmente en los casos que se identifican nuevos riesgos, cuando es necesario rediseñar los controles existentes o definir unos nuevos controles.

9. CRONOGRAMA

GOBERNACIÓN DE ANTIOQUIA
República de Colombia

ACTIVIDADES/ ACCIONES A DESARROLLAR	PRODUCTO	META PROGRAMADA	RESPONSABLE	1 TRIMESTRE			2 TRIMESTRE			3 TRIMESTRE			4 TRIMESTRE		
				Ene	Fer	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Revelar información sensible o confidencial para beneficio propio o de un tercero. - Divulgar y gestionar el cumplimiento de la política de seguridad digital.	Documento de seguimiento	100%	Ingeniero de Sistemas – Líder Sistemas						1					1	
Revelar información sensible o confidencial para beneficio propio o de un tercero. - Construir la Matriz de Clasificación y Registro de Activos de Información	Documento de matriz y clasificación	100%	Ingeniero de Sistemas – Líder Sistemas – Técnica en Gestión documental											1	
Revelar información sensible o confidencial para beneficio propio o de un tercero. - Verificar la adecuada definición e implementación de los esquemas de perfiles de acceso a la información definidos.	Documento de seguimiento	100%	Ingeniero de Sistemas – Líder Sistemas						1						
Destrucción de información con fines ilícitos. - Generar y divulgar un Protocolo	Documento de seguimiento	100%	Ingeniero de Sistemas – Líder Sistemas			1									

de acceso al centro de datos de la entidad															
Destrucción de información con fines ilícitos. - Verificar la adecuada definición e implementación de los esquemas de perfiles de acceso a la información definidos.	Documento de seguimiento	100%	Ingeniero de Sistemas – Líder Sistemas						1						
Destrucción de información con fines ilícitos. - Validar la correcta y adecuada toma de copias de respaldo	Documento de seguimiento	100%	Ingeniero de Sistemas – Líder Sistemas				1			1				1	
Fuga de información - Verificar la adecuada definición e implementación de los esquemas de perfiles de acceso a la información definidos.	Documento de seguimiento	100%	Ingeniero de Sistemas – Líder Sistemas						1						
Fuga de información - Validar la correcta y adecuada toma de copias de respaldo	Documento de seguimiento	100%	Ingeniero de Sistemas – Líder Sistemas				1			1				1	
Ataque cibernético sobre la plataforma tecnológica - Revisión periódica de controles para evitar pérdida de información.	Documento de seguimiento	100%	Ingeniero de Sistemas – Líder Sistemas				1			1				1	
Ataque cibernético sobre la plataforma tecnológica - Validar la	Documento de seguimiento	100%	Ingeniero de Sistemas – Líder Sistemas				1			1				1	

correcta y adecuada toma de copias de respaldo.															
Ataque cibernéticosobre la plataforma tecnológica - Mantener actualizado y vigente el esquema de seguridad perimetral definido.	Documento de seguimiento	100%	Ingeniero de Sistemas – Líder Sistemas						1					1	
Ataque cibernéticosobre la plataforma tecnológica - Mantener actualizado y vigente el esquema de antivirus definido.	Documento de seguimiento	100%	Ingeniero de Sistemas – Líder Sistemas							1					
Inadecuado tratamiento de datos personales - Validar que se cuente con definiciones y políticas de seguridad digital que aseguren la privacidad y la protección de los datos personales, de acuerdo con los lineamientos internos para la calificación de la información y las disposiciones generales que exige la legislación nacional.	Documento de seguimiento	100%	Ingeniero de Sistemas – Líder Sistemas											1	

10. RESPONSABLE

Subgerencia administrativa
Líder de sistemas

11. MEDICION

Medición de adherencia política de seguridad y privacidad de la información

Indicador:

$\frac{\text{Número de pruebas realizadas}}{\text{Número total del personal invitado}} \times 100$	Medir la adherencia del personal invitado para la política de seguridad y privacidad de la información.

RANGO		
0-60%	Rojo	Baja
61-89%	Amarillo	Media
90-100%	Verde	Alta

12. SEGUIMIEMTO

Trimestral

13. ELABORADO POR:

CARLOS ANDRES MUÑOZ VELEZ
Ingeniero de Sistemas