MODELO DE SEGURIDAD YPRIVACIDAD DE LAINFORMACION

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El modelo de seguridad y privacidad de la información MSPI, mantiene la importancia de perseverar en la seguridad de los datos y contribuye a la minimización de riesgos relacionados con pérdidas, hace más eficiente la gestión y asegura el cumplimiento de las labores de Contexto del Instituto de Cultura y Turismo de Bolívar, apoyando el uso adecuado de las TIC.

El nivel de seguridad y privacidad de la información ha sido establecido por el Gobierno Nacional en cabeza del Ministerio de Tecnologías de Información y las Comunicaciones – MinTIC para las entidades públicas a través de la Resolución 746 del 11 de marzo de 2022, "por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021". *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad de la Información como habilitador de la política de Gobierno Digital"*. Es por eso que el MinTIC establece lineamientos con el objetivo de generar confianza en el uso del entorno digital, garantizando el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en las Entidades Públicas.

2. JUSTIFICACIÓN

El presente documento "Modelo de seguridad y privacidad de la información - MSPI" es importante pues establece la confidencialidad, integridad y disponibilidad de los datos, lo que permite asegurar la privacidad de estos a través del proceso de gestión de riesgos y da confianza a las partes interesadas de la correcta gestión de riesgos.

3. OBJETIVO GENERAL.

Implementar la norma NTC/IEC ISO 27001:2022, estrategia de gestión digital, política nacional de seguridad digital, CONPES 3854 seguridad de datos y actividades de planificación de privacidad de acuerdo con las leyes disponibles vigentes.

3.1 Objetivos Específicos

- Mantener instrucciones para el manejo de la información digital como parte de la seguridad y privacidad de la información.
- Utilizar la implementación del sistema de gestión de seguridad de la información del Instituto de Cultura y Turismo de Bolívar de acuerdo a los requisitos estipulados en el modelo de seguridad y privacidad de la información de acuerdo con los estándares requeridos en la estrategia de gobierno digital.
- Gestionar los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad del negocio.
- Reducir las interrupciones en la seguridad y privacidad de los datos, seguridad digital de manera efectiva, eficiente y eficaz.
- Crear conciencia sobre los cambios organizacionales necesarios para implementar la seguridad y privacidad de los datos como un enfoque central para el Instituto de Cultura y Turismo de Bolívar.
- Cumplir los requisitos derivados de la ley sobre seguridad y privacidad de la información, seguridad digital y protección de datos personales.

4. MODELO DE SEGURIDAD MSPI

El modelo de seguridad y privacidad de MSPI de la estrategia de gobierno digital explora los siguientes ciclos de acción, que incluyen cinco (5) pasos para permitir que las entidades gestionen adecuadamente la seguridad y la privacidad de sus activos de información.

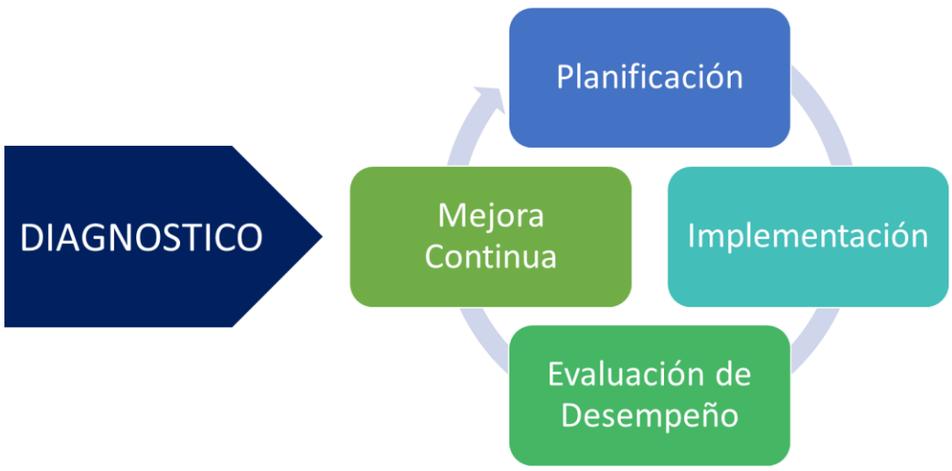

Figura 1 Ciclo de operación Modelo de Seguridad y Privacidad de la Información Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

Figura 2. Fases MSPI http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

5. FASE DE DIAGNOSTICO

Esta etapa de DIAGNÓSTICO según ISO 27001:2022 en el Capítulo 4 - Contexto Organizacional determina la necesidad de analizar los problemas externos e internos del Instituto de Cultura y Turismo de Bolívar y su contexto, incluye los requisitos y expectativasde las partes interesadas de la organización para lograr el alcance del SGSI.

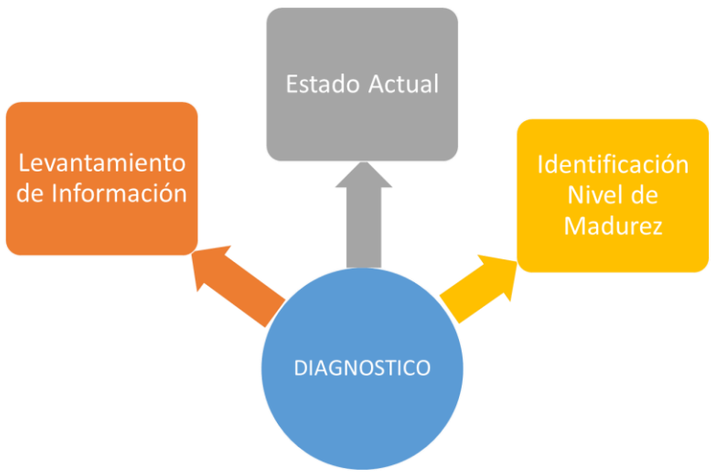

Figura 3 Etapas previas a la implementación Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pd

5.1 ESTADO ACTUAL DEL INSTITUTO DE CULTURA Y TURISMO DE BOLÍVAR

5.1.1 Conocimiento del Instituto

5.1.1.1 Misión

Garantizar a sus habitantes una oportuna y efectiva prestación de los servicios con calidad en materia de salud, educación, seguridad, construcción de obras de infraestructura, ordenamiento territorial, medio ambiente, crecimiento socio – cultural, deportivo y erradicación de la pobreza, promoviendo la participación comunitaria en aras de mejorar la calidad de vida de nuestros ciudadanos y de quienes visitan nuestro territorio.

5.1.1.2 Visión

En el año 2027 el Instituto de Cultura y Turismo de Bolívar será líder en desarrollo sostenible caracterizada por una cultura emprendedora, empoderada del medio ambiente, participativa, solidaria yorgullosa de su patrimonio e historia.

5.1.1.3 Valores Éticos

Son formas de ser y actuar de las personas que son altamente deseables como atributos o cualidades nuestras y de los demás, por cuanto posibilitan la construcción de una convivencia gratificante en el marco de la dignidad humana.

Responsabilidad: Obligación de responder por los propios actos. Capacidad para reconocer y hacerse cargo de las consecuencias de las propias acciones.

Respeto: Miramiento, consideración, deferencia del otro. Reconocimiento de la legitimidad del otro para ser distinto de uno.

Honestidad: Moderación en la persona, las acciones o las palabras. Honradez, decencia. Actitud para actuar con honradez y decencia.

Transparencia: Se refiere al comportamiento claro, evidente, que no deja dudas y que no presenta ambigüedad. Es lo contrario de la opacidad, que no deja ver, que esconde. Se sitúa en el ámbito de la comunicación, del suministro de información, de la rendición de cuentas a la sociedad.

5.1.1.4 Organización del Instituto de Cultura y Turismo de Bolívar

5.2 IDENTIFICACION DEL NIVEL DE MADUREZ

Se utilizó la herramienta de evaluación MINTIC MSPI para identificar el nivel de madurez en seguridad y privacidad de la información del Instituto de Cultura y Turismo de Bolívar , la cualarrojó el siguiente resultado:

Figura 4- Nivel de madurez en seguridad y privacidad de la información.

Figura 5- Niveles de madurez Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

5.3 LEVANTAMIENTO DE INFORMACIÓN

Son partes interesadas del Instituto de Cultura y Turismo de Bolívar, las entidades públicas yprivadas legalmente constituidas, que interactúan con la misma; teniendo presente los requisitos normativos internos, legales o reglamentarios y las obligaciones contractuales.

PARTES INTERESADAS	DEFINICION
GOBIERNO	**MINISTERIO DE LAS TIC**
	Órganos de control, Ministerio de las Tic, Función Pública, Contraloría General de la Republica entre otras.
FUNCIONARIOS	**Funcionarios de Planta o Provisionales**: Personas vinculadas a la entidad bajo una relación legal y reglamentaria para el cumplimiento de funciones administrativas u otras en el marco de personal aprobada.
	Contratistas: Personas naturales que apoyan a las que trabajan en la Alcaldía de actividades del que hacer propio y misional de la Institución (Alcaldía) mediante la modalidad de prestación de servicio.
PROVEEDORES	Persona Natural, jurídica u organización que tiene vínculo contractual con el Instituto, para suministrar bienes, obras o servicios.
COMUNIDAD	Ciudadanos que están interesados en la misión propia de la institución.

Tabla 1 Partes Interesadas

Figura 6. Mapa de procesos

https://icultur.gov.co/Documentos/Transp_estructura-organica/D4762996-BEDB-45A9-87C5-F484BDA96B8F.jpeg

5.3.1 Clasificación de Activos de Información

6. FASE DE PLANIFICACIÓN

Esta fase de PLANIFICACIÓN que cumple con ISO 27001:2022 en el Capítulo 5 - Liderazgo, define las responsabilidades y obligaciones de la alta dirección en relación con el sistema de gestión de seguridad de la información, incluida la necesidad de que la alta dirección prepare una política de seguridad de la información adecuada a la alcaldía, que asegura la distribución de los recursos del SGSI, la distribución, comunicación de responsabilidades y roles importantes desde el punto de vista de la seguridad de la información.

En el capítulo 6 – Planificación, se establecen los requerimientos para la valoración y tratamiento de riesgos de seguridad, la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.

En el Capítulo 7 – Soporte, se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua del Sistema de Gestión de Seguridad de la Información.

Figura 7. Fase de planificación Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

6.1 Contexto del Instituto de Cultura y Turismo de Bolívar.

6.1.1 Generalidades

El Instituto de Cultura y Turismo de Bolívar es una entidad territorial que forma parte de la organización territorial de la República y tiene autonomía política, fiscal y administrativa para gestionar sus intereses dentro de los límites de la Constitución y la ley y con base enla política TIC de la República. ámbito relacionado con la política de gobierno digital del Gobierno Nacional, establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic) y normativa de planificación del sector TIC.

A través del Modelo de Seguridad y Privacidad de la información - MSPI, mediante su implementación se crea una estrategia integral de seguridad de la información, la cual se implementa de manera integrada con el sistema de gestión de seguridad de la información, debido a que la norma ISO/IEC 27001:2013 se basa en ambos sistemas y los lineamientos técnicos desarrollados por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, que brindan apoyo integral a otras áreas de la estrategia de gobierno digital: TIC para el Estado y TIC para la sociedad.

6.1.2 Contexto Tecnológico

Conexiones: La conectividad del conjunto está asegurada mediante un canal propio de fibra óptica, que posibilita la conexión con diversas instituciones del municipio. De esta forma, el canal de comunicación puede soportar las necesidades del conjunto. El Instituto, considerando la infraestructura física, la cantidad de oficinas y personal que allí trabaja, así como la planta y los contratistas, requiere una arquitectura de conectividad híbrida para operar, es decir. debe tener conectividad por cable e inalámbrica, también se deben definir los tipos de perfiles de uso de la red Wi-Fi.

Red local: La red local (LAN) debe garantizar que la red de fibra óptica llegue a la red troncal y pueda distribuirse con al menos cableado categoría 5e en cada

ubicación. El análisis de segmentos se realizó según el número de oficinas administrativas. LAN inalámbrica: Se realizará una revisión para optimizar la calidad del diseño actual de la red Wi-Fi, la cual deberá incluir el perfilamiento de los usuarios para su uso y gestión. Los cambios de contraseña también se producen periódicamente.

Canal Internet: El servicio está diseñado para brindar tráfico de Internet saliente y entrante para toda la unidad, oficinas y áreas Wi-Fi.

6.1.3 Expectativas de las Partes Interesadas

Partes Interesadas	Necesidades	Requisitos	Solicitud	Expectativas
Administraci Municipal GOBIERNO	Contar con la información en los plazos establecidos	Disposición de recursos financieros para la implementación del MSPI Cumplir con la normatividad aplicable Definir directrices y políticas ajustadas a las condiciones operacionales de la Alcaldía	Determinar las normas aplicables para el MSPI	Cumplir con los requerimientos y las directrices establecidas por los diferentes entes Gubernamentales.
				Mejorar la imagen de la institucionalidad e incrementar el nivel de competitividad
FUNCIONARIOS	Contar con herramientas tecnologías aprobadas	Apoyo tecnológico que permita seguir las directrices establecidas del SGSI	Políticas de Seguridad	Aprobación del SGSI, a través de aplicación de la políticas.
		Disponibilidad del servicio	Acuerdo de confidencialidad	Obtener Integridad y confidencialidad de la información

		Disponibilidad del servicio	Documentos del MSPI	Obtener una disponibilidad de los servicio Cumplimento de los acuerdos de nivel de servicio
PROVEEDORES	Especificaciones técnicas de lo requerido, acorde a las políticas de seguimientos del SGSI.	Cumplimiento en tiempos de entrega pactados.	Acuerdo de confidencialidad con terceros	Minimizar el riesgo del uso. inadecuado de la información
			Política de seguridad actualizada	Proteger con todo los controles de seguridad
COMUNIDAD	Información	Transparencia en el desarrollo de los procesos institucionales del Instituto	Aplicar las directrices establecidas por gobierno digital	Facilitar el acceso a la información pública de manera permanente (transparencia y acceso a la información) ley 1712
		Consistencia y veracidad de la información suministrada por la institución		

Tabla 2 Expectativas Partes Interesadas

6.1.4 Alcance del MSPI

Alcance del Modelo de Seguridad y Privacidad de la Información - Instituto de Cultura y Turismo MSPI aplica a todos los procesos, funcionarios, proveedores, contratistas, comunidad y quienes comparten, usan, recaudan, procesan de acuerdo a sus funciones, intercambiar o consultar información y monitorear entidades o sujetos que tengan acceso interno o externo a cualquier tipo de información sin importar su ubicación; De esta manera, nuestro objetivo es proteger y preservar la integridad ydisponibilidad de los activos de información.

6.2 Liderazgo

6.2.1 Liderazgo y Compromiso de la Alta Dirección

El Instituto de Cultura y Turismo de Bolívar se compromete a liderar la implementación del MSPI, y a gestionar la asignación de los recursos necesarios para garantizar la seguridad de la información del Instituto, delegando en la Oficina TIC, la responsabilidad de la elaboración, implementación, seguimiento y a los planes, para mejorar el modelo de seguridad y privacidad de la información.

6.2.2 Política de Seguridad

El Instituto de Cultura y Turismo de Bolívar entendió la importancia de una adecuada gestión de la información y apuesta por la implementación de un sistema de gestión de seguridadde la información que tenga como objetivo crear un marco confidencial para el cumplimiento de sus deberes con el Estado y la ciudadanía, estrictamente de acuerdo con la ley y de acuerdo con la misión y visión de la unidad. Para el instituto, el objetivo de la protección de la información es reducir sistemáticamente el impacto de los riesgos identificados en nuestros activos para mantener un nivel deexposición que nos permita ser responsables de la integridad, confidencialidad ydisponibilidad de la información, seguridad de información, según las necesidadesde los distintos grupos de interés.

Como se indicó anteriormente, este modelo de seguridad y privacidad de la información, aplica a la Administración, sus empleados, terceros, pasantes, practicantes, proveedores y ciudadanía en general, siempre que los principios por los cuales las acciones o decisiones relacionadas con el SGSI estén determinadas por lo siguiente:

- Cumplimiento de los principios de seguridad de la información.
- Mantener la confianza de la ciudadanía, aliados y empleados.
- Apoyar la innovación tecnológica.
- Protege los activos tecnológicos.
- Preparar principios, procedimientos e instrucciones sobre seguridad de la información.
- Fortalecer la cultura de seguridad de la información del instituto.
- Asegurar la continuidad del negocio ante eventos e incidencias.
- El instituto decidió definir, implementar, utilizar y mejorar continuamente un sistema de gestión de seguridad de la información sustentado en lineamientos claros de acuerdo a las metas planteadas en el Plan de Desarrollo y la normatividad. (MinTIC, 2022)

6.2.3 Roles y Responsabilidades (Anexo. 2 Documento de Gestión de Roles y responsabilidades MSPI)

RECURSO HUMANO	Funcionarios responsables	ROL	RESPONSABILIDADES
COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	JEFES DE AREA (Secretarios, Directores, Jefes de Oficina)	Alta Dirección	Aprobación del MSPI y de la Gestión de roles y responsabilidades. Apoyo implementación MSPI Gestión Estratégica
COMITÉ DE SEGURIDAD DE LA INFORMACION	CONTROL INTERNO DISCIPLINARIO, AREA JURIDICA, PLANEACION, GESTION DE CALIDAD, CONTRATACION, OFICINA ASESORA DE COMUNICACIÓN, PRENSA Y PROTOCOLO, OFICINA TIC.	Toma de decisiones.	Toma de decisiones frente a la seguridad de la Información

LIDER DE TECNOLOGÍA	JEFE DE OFICINA TIC	Responsable MSPI.	Liderazgo y responsabilidad del MSPI Gestión estratégica y táctica
PARTES INTERESADAS.	TODAS LAS SECRETARIAS/DEPENDENCIAS DE LA ADMINISTRACION MUNICIPAL	Cumplimiento MSPI.	Dar estricto cumplimiento a lo estipulado en el MSPI.
FUNCIONARIOS SOPORTE TECNICO Y ESPECILIZADO.	MESA DE AYUDA	Apoyo operativo de las actividades requeridas del MSPI	Gestión operativa y apoyo al Oficial de Seguridad de la Información o quien haga sus veces y Especialista de Seguridad Informática.
ESPECIALISTA SEGURIDAD INFORMATICA.	OPS o Funcionario de Planta OFICINA TIC	Apoyo operativo de las actividades requeridas del MSPI	Gestión operativa y apoyo al Oficial de Seguridad de la Información o quien haga sus veces.
GRUPO DE INFRAESTRUCTURA TECNOLOGICA	OPS o Funcionario de planta OFICINA TIC	Gestión de la transición y migración IPv4 a IPv6 Ejecución de actividades del MSPI	Implementar las estrategias de apropiación de los servicios tecnológicos
GRUPO DE DESARROLLO DE SISTEMAS DE INFORMACIÓN	Líder del área de desarrollo y OPS	Ejecución de actividades del MSPI	Implementar estrategias de seguridad en los sistemas de información desarrollados por la Oficina TIC

Tabla 3. Roles y responsabilidades

Responsabilidades:

- ✓ Generar análisis y evaluación de riesgos TIC.
- ✓ Identificación de riesgos TIC.
- ✓ Incorporación de la gestión de riesgos TIC.
- ✓ Evaluación de tratamiento de riesgos TIC.
- ✓ Validar la implementación y operación del SGSI y MSPI.
- ✓ Implementación del plan de tratamiento de riesgos TIC para lograr los objetivos de control identificados.

7. GLOSARIO

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

Amenaza: causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

Amenaza informática: la aparición de una situación potencial o actual donde una persona tiene la capacidad de generar una agresión cibernética contra la población, el territorio, la organización política del Estado (Ministerio de Defensa de Colombia).

Análisis de riesgos: proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.

Anonimización del dato: eliminar o sustituir algunos nombres de personas (físicas o jurídicas); direcciones y demás información de contacto, como números identificativos, apodos o cargo.

Autenticidad: propiedad de que una entidad es lo que afirma ser. (ISO 27000.es, 2012).

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

Ciberespacio: ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).

Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control: comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

Custodio de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la Veeduría Distrital, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad. Datos abiertos: son datos primarios o sin procesar puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos biométricos: parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (huella digital o voz).

Dato privado: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato semiprivado: es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

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

Dato público: es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato semiprivado: es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Backbone: troncal (en inglés *backbone*), red troncal o troncal de internet, es una de las principales conexiones de internet.

DVD: Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.

Disco duro: disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y regrabados como una cinta de audio.

Evento de seguridad de la información: ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

Gestión de claves: son controles que realizan mediante la gestión de claves criptográficas.

Gestión de riesgos: actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Impacto: el coste para la empresa de un incidente -de la escala que sea, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

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.

Habeas data: derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

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.

Integridad: la propiedad de salvaguardar la exactitud y complejidad de la información.

Información: La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser

Integridad: la propiedad de salvaguardar la exactitud y complejidad de la información.

No repudio: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).

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

Plan de 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.

Plan de continuidad del negocio: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Proceso: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012)

Propietario de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

Responsable del tratamiento: persona natural o jurídica, pública o privada. Que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información (SGSI): conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

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.

Vulnerabilidad: debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

Política de Firewall: Una Política de Firewall es una de las herramientas más importantes a la hora de configurar un firewall, ya que a través de ciertas configuraciones que el administrador realice, según la necesidad de la empresa, se puede determinar el comportamiento del dispositivo en la red.

1. REFERENCIAS

Mintic. (25 de 04 de 2022). *mintic.gov.co*. Obtenido de mintic.gov.co: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-162621_Modelo_de_Seguridad_y_Privacidad____MS

https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf


icultur
INSTITUTO DE CULTURA Y TURISMO DE BOLÍVAR


icultur
INSTITUTO DE CULTURA Y TURISMO DE BOLÍVAR

protegidos de potenciales riesgos. (ISO 27000.es, 2012)


icultur
INSTITUTO DE CULTURA Y TURISMO DE BOLÍVAR