PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UAESP
Enero 2023

ALCALDÍA MAYOR DE BOGOTÁ D.C.
UAESP
Unidad Administrativa Especial de Servicios Públicos
BOGOTÁ

Comité Institucional de Gestión y Desempeño

Director(a) General
Jefe(a) Oficina Asesora de Planeación
Jefe(a) Oficina Asesora de Comunicaciones
Jefe(a) Oficina de Tecnologías de Información y Comunicaciones
Jefe(a) Oficina de Control Interno Disciplinario
Subdirector(a) Administrativo y Financiero
Subdirector(a) Asuntos Legales. Subdirector(a) Recolección Barrido y Limpieza.
Subdirector(a) Aprovechamiento
Subdirector(a) Disposición Final
Subdirector(a) Servicios Funerarios y Alumbrado público.

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

TÉRMINOS Y DEFINICIONES

Activos de información: Toda información o elemento relacionado con el tratamiento de esta (Documentos, hardware, software, servicios, edificios, personas, entre otros) que tenga valor para la organización y por lo tanto se debe proteger. Se puede considerar un activo de información los datos creados o utilizados por un proceso, pueden ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, equipos de cómputo relacionados al tratamiento o almacenamiento de información, software del sistema, servicios utilizados para la transmisión, recepción y control de la información, entre otros.

Administración de Riesgos: Conjunto de elementos de control que al interrelacionarse permiten a la Entidad Pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función.

Amenaza: Causa potencial de un incidente no deseado que puede provocar daños o afectaciones aun activo de información.

Autoridad competente: Es la autoridad apta e idónea para tratar de un determinado procedimiento o proceso de acuerdo con la ley.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [ISO 27000].

Disponibilidad: La propiedad de tener la información cuando es requerida. Se relaciona con la facilidad y oportunidad de acceso a la información.

Evaluación del Riesgo: Permite comparar los resultados de su calificación, con los criterios definidos para establecer el grado de exposición de la entidad al riesgo; de esta forma es posible distinguir entre los riesgos ubicados en los niveles: Nivel bajo, moderado, alto y extremo y fijar prioridades de las acciones requeridas para su tratamiento.

Evento de seguridad de la información: Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la Política de Seguridad de la Información o falla en los controles.

Incidente de seguridad de la información: Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones de la Entidad y de amenazar la seguridad y privacidad de la información.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas

o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Integridad: Propiedad de la información relativa a su exactitud y completitud. [ISO 27000].

MSPI: Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones – MinTIC.

Partes Interesadas: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
Es pertinente señalar que "seguridad de la información" no solo corresponde a Seguridad Informática, sino que su alcance se complementa con ciberseguridad, seguridad física, ambiental y del recurso humano entre otras, buscando mantener la confidencialidad, la disponibilidad e integridad de la información. [Directiva 002 de 2021 – Alcaldía Mayor de Bogotá].

Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

SGSI: Sistema de Gestión de la Seguridad de la Información.

Sistema de información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

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

Usuario: Cualquier persona que tiene acceso a la plataforma y a los activos de información, sea en calidad de usuario final, tercero o administrador de la plataforma.

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

1. INTRODUCCIÓN

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

La implementación del plan de Seguridad y Privacidad de la Información en la Entidad está determinada por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de esta, todo con el objetivo de preservar la confidencialidad, integridad y disponibilidad de los activos de información.

2. OBJETIVO

Establecer las actividades que permitan incrementar el nivel de madurez del Modelo de Seguridad y Privacidad de la Información implementado en la UAESP a “Optimizado” en el marco del modelo de referencia definido por el Ministerio de Tecnologías de la Información – MINTIC y con base en el modelo PHVA (Planear-Hacer- Verificar-Actuar) definido en la norma NTC/IEC ISO 27001:2013 y el Sistema de Gestión de la Seguridad de la Información (SGSI).

2.1 Objetivos Específicos

- Adelantar revisiones al MSPI con el fin de verificar el funcionamiento y cumplimiento normativo.
- Fortalecer los procedimientos y controles relacionados con el Modelo de Seguridad de la Información.
- Dar cumplimiento a la normatividad vigente en materia de Seguridad y Privacidad de la Información.
- Aumentar el porcentaje de implementación de controles del Modelo de Seguridad y Privacidad de la Información en la Entidad.

3. REFERENCIA NORMATIVA

- CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital.
- Decreto 103 de 2015 el cual reglamenta la ley 1712 de 2014 "Ley de Transparencia “.
- Ley 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 de 2013 y por el Decreto 1081 de 2015, “Protección de datos personales”.
- Decreto único reglamentario 1078 de 2015 – MinTic – Modelo de Seguridad y Privacidad de Información.
- ISO/IEC 27000:2013. Estándar del Sistema de Gestión de Seguridad de Información.
- Resolución 1519 de 2020: Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- Resolución 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 como habilitador de la política de seguridad y privacidad de la información y el manual de políticas de seguridad de la información.
- Decreto 767 de 2022: "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”.

4. RESPONSABLES DE LA IMPLEMENTACIÓN

Se adopta al interior de la Entidad la Resolución 313 de 2020 “Por medio de la cual se establecen las instancias de operacionalización del Sistema de Gestión y Sistema de Control Interno en la Unidad Administrativa Especial de Servicios Públicos, y se define otros lineamientos”.

Artículo 2° CREACIÓN DEL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO DE LA UNIDAD ADMINISTRATIVA ESPECIAL DE SERVICIOS PÚBLICOS. Créase el Comité Institucional de Gestión y Desempeño en la Unidad Administrativa Especial de Servicios Públicos (UAESP), encargado de orientar la implementación y seguimiento del Sistema de Gestión y la operación del MIPG, articulando todos los procesos y actividades de la UAESP, recursos, herramientas, estrategias y políticas de gestión y desempeño institucional, de acuerdo con la normatividad vigente en la materia.

Artículo 32°. MESAS TÉCNICAS DE TRABAJO. Con el fin de garantizar el óptimo funcionamiento del Comité Institucional de Gestión y Desempeño, del Comité Institucional de Coordinación de Control Interno de la UAESP y el de facilitar la implementación y desarrollo del Modelo Integrado de Planeación y Gestión, se podrán conformar mesas técnicas de trabajo necesarias para operacionalizar las Políticas del MIPG vigentes en la UAESP.

Por lo anterior, y de acuerdo con las funciones descritas del Comité Institucional de gestión y Desempeño en el artículo 4, es responsabilidad de la Dirección velar por la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI- mediante el aseguramiento de la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad y privacidad de la información.

Así mismo, la Oficina TIC como líder de la Política de Seguridad Digital, a través de la mesa técnica de Seguridad Digital hará seguimiento a la Implementación del Modelo de Seguridad y Privacidad de Información – MSPI en la Entidad.

5. ALCANCE

Aplica a todos los procesos de la UAESP, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información, el cual hace parte del Sistema Integrado de Gestión de la UAESP.

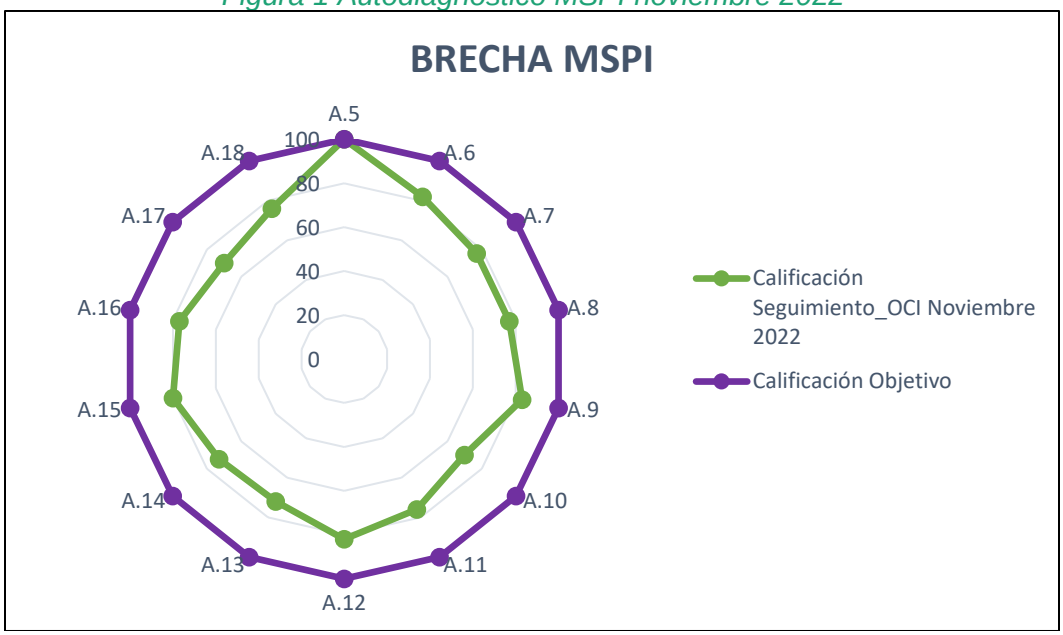
6. ANÁLISIS DE BRECHA

El análisis de brecha busca generar un diagnóstico de la seguridad de la información basado en la identificación de diferencias entre el estado actual y el estado deseado de la Unidad Administrativa Especial de Servicios Públicos de acuerdo con los requerimientos exigidos por el Modelo de Seguridad y Privacidad de la Información - MSPI y las consideraciones definidas internamente como parte del ejercicio de la Entidad y el cumplimiento de su misionalidad.

La Entidad hace uso de la herramienta diseñada por el MinTIC para autoevaluar la implementación y el nivel madurez del MSPI y las evaluaciones realizadas por la Oficina de

Control Interno en noviembre de 2022, para tener una perspectiva más amplia en relación con el avance a la fecha y junto a la brecha encontrada, definir la hoja de ruta y las acciones a desarrollar para la implementación del MSPI y alcanzar las metas definidas por el MinTIC a través del Decreto 1078 de 2015

Figura 1 Autodiagnóstico MSPI noviembre 2022



Fuente: Propia

Como resultado de la última auditoria efectuada al Modelo de Seguridad y Privacidad de la Información, se obtuvo una calificación cuantitativa promedio de controles implementados del 78%.

El plan busca llevar a la Entidad un nivel de madurez del MSPI "**Optimizado**" implementando el 100% de los controles definidos en el MSPI.

7. HOJA DE RUTA

De acuerdo con el análisis de la brecha encontrada del Modelo implementado en la Entidad, la Política General, el Manual de Seguridad y Privacidad de la Información y las acciones definidas en el plan de mejoramiento del proceso de gestión tecnológica y de la información, se definen las siguientes actividades para incrementar los niveles de madurez y controles definidos en el MSPI.

Tabla 1 Hoja de ruta implementación MSPI

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA INICIO	FECHA FIN
Política de seguridad de la información (A.1)	1	Revisar la conveniencia de la política general de seguridad y privacidad de la información.	Política actualizada. Nota: En caso de no requerir actualización por ser aún	Oficial de Seguridad de la Información.	01/02/2023	31/05/2023

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA INICIO	FECHA FIN
			oportuna, socializar en mesa de seguridad digital y entregar acta de reunión donde se evidencia la revisión y adecuación.			
	2	Realizar autodiagnóstico.	Autodiagnóstico e informe con recomendaciones presentado en la Mesa Técnica de seguridad Digital	Oficial de Seguridad de la información	01/02/2023	31/05/2023
Organización de la seguridad de la información (A.2)	3	Definir los lineamientos para la inclusión de la seguridad y privacidad de la información en la metodología de proyectos que tenga la Entidad. Nota: Contemplar Activos que se involucren en el proyecto, información confidencial y riesgos de seguridad de la información y otros que apliquen.	Circular o documento pertinente con los lineamientos.	Oficina Asesora de Planeación	01/02/2023	30/04/2023
	4	Realizar divulgación de la Política General de Seguridad y Privacidad de la Información, incluyendo roles y responsabilidades en seguridad de la información.	Asistencia y evaluación de la divulgación.	Oficial de Seguridad de la Información / OTIC	01/02/2023	30/04/2023
Seguridad de los recursos Humanos (A.3) Seguridad de los recursos Humanos (A.3)	5	Definir acuerdos de confidencialidad en relación con las responsabilidades de los servidores (as) públicos (as) y la UAESP con la seguridad y privacidad de la información. Nota: Se deberá incluir los tiempos de cobertura (Antes, Durante y Después), responsabilidades, uso permitido de la información, notificación en caso de incidentes o fugas de información y acciones en caso de incumplimiento.	1. Formato de Acuerdo de confidencialidad incorporado al Procedimiento de vinculación de personal. 2. Acuerdos de confidencialidad del personal de planta activo diligenciados, firmados e incorporados en los expedientes laborales	Subdirección Administrativa y Financiera – Talento Humano	01/02/2023	30/04/2022
	6	Formular o actualizar el plan de sensibilizaciones y	Plan aprobado.	Oficial de Seguridad de la Información.	01/02/2023	31/03/2023

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA INICIO	FECHA FIN
		capacitaciones de seguridad y privacidad de la información 2023, alineado con el Plan Anual de Capacitaciones.				
Gestión de Activos de información (A.4)	7	Revisar o actualizar, de ser necesario, los lineamientos para el inventario de activos de información.	Procedimiento o lineamientos actualizados. Nota: Si no se requiere actualización, acta de reunión de la revisión.	OTIC / Gestión Documental / Oficial de Seguridad de la Información.	01/02/2023	28/02/2023
	8	Realizar la actualización del inventario de activos de información.	Inventario de activos de información aprobado por la Dirección.	Todos los procesos	01/02/2023	31/10/2023
	9	Implementar los lineamientos para el etiquetado de información.	Muestra de información física y Digital etiquetada	Todos los Procesos	01/02/2023	31/10/2023
	10	Revisar la aplicación de controles de seguridad para medios removibles.	Informe de controles aplicados sobre dispositivos de almacenamiento removible.	OTIC	01/02/2023	30/04/2023
Continuidad del Negocio (A.5)	11	Ejecutar el plan de pruebas de continuidad del negocio.	Informe y recomendaciones para la mejora o actualización del Plan de continuidad del negocio, de acuerdo con el resultado del plan de pruebas presentados a la mesa técnica de seguridad digital. Informe del plan de pruebas del DRP ejecutado y recomendaciones, cuando apliquen. Nota: El informe deberá estar consolidado en el informe del plan de continuidad del negocio.	OAP / OTIC	01/02/2023	31/05/2023
Cumplimiento (A.6)	12	Sensibilizar la política y el Manual de Protección de Datos Personales.	Asistencia y evaluación de la divulgación.	Oficial de Datos Personales	01/02/2023	01/05/2023
	13	Elaborar el plan de pruebas de penetración 2023.	Plan Aprobado	Oficial de Seguridad de la información /	01/02/2023	31/03/2023

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA INICIO	FECHA FIN
				OTIC		
Control de Acceso (T.1)	14	Realizar revisión de derechos de acceso a los sistemas de información de acuerdo con el procedimiento de gestión de usuarios.	Informe o comunicaciones oficiales.	OTIC en conjunto con todos los Procesos.	01/02/2023	31/12/2023
	15	Implementar mecanismo de autogestión de contraseñas	Informe aprobado por el jefe de la OTIC donde se verifique la implementación.	OTIC	01/02/2023	31/10/2023
	16	Realizar campañas para la autogestión de contraseñas dentro del dominio de la Entidad.	Campañas, piezas comunicativas o listados de asistencia.	OTIC	01/02/2023	31/10/2023
Criptografía (T.2)	17	Aseguramiento de conexiones entre aplicación y base de datos.	Informe aprobado por el jefe de la OTIC.	OTIC	01/02/2023	31/03/2023
	18	Definir lineamientos para el uso de firmas mecanografiadas, digitales o electrónicas en la Entidad.	Lineamiento, directriz o documento equivalente.	Gestión Documental	01/02/2023	30/04/2023
	19	Sensibilizar a servidores (as) públicos (as) y contratistas de la Entidad sobre la política de cifrado de la información y uso de controles criptográficos, incluyendo la responsabilidad de los usuarios.	Listados de Asistencia y evaluación.	OTIC	01/02/2023	30/04/2023
Seguridad Física y del Entorno (T3)	20	Definir controles de seguridad física para las áreas seguras de la Entidad.	Listado de las áreas seguras y verificación de controles de acceso implementados de acuerdo con el ítem T3.1.1 y T3.1.5 del autodiagnóstico del MSPI	Apoyo Logístico	01/02/2023	30/04/2023
	21	Revisión de riesgos ambientales y amenazas externas.	Riesgos y Controles de mitigación documentados.	OAP	01/02/2023	31/03/2023
	22	Revisión de las condiciones del cuarto eléctrico.	Informe de las condiciones y recomendaciones para el cuarto eléctrico.	OTIC	01/02/2023	31/10/2023
	23	Definir los lineamientos para el retiro de activos de información de la Entidad.	Lineamientos documentados y aprobados por la SAF / Dirección.	SAF – Apoyo logístico	01/02/2023	28/02/2023
	24	Definir puntos de control para la	Lineamientos o documentos aprobados.	OTIC / Apoyo Logístico	01/03/2023	31/04/2023

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA INICIO	FECHA FIN
		disposición segura de medios de almacenamiento de la Entidad.				
Seguridad en las Operaciones (T.4)	25	Probar el proceso de restauración de respaldos de forma periódica.	Cronograma e informes y recomendaciones de las pruebas ejecutadas.	OTIC	01/02/2023	31/12/2023
	26	Ajustar el correlacionador de evento, incluyendo los logs de los diferentes sistemas de seguridad.	Reportes o informes mensuales con el análisis del correlacionador de eventos y la definición del almacenamiento de los logs que mitigue los errores por sobrepasar su capacidad u otra limitante. Nota: De no ser posible lo anterior, se debe documentar el análisis de los reportes de las diferentes herramientas de seguridad.	OTIC	01/02/2023	31/05/2023
	27	Documentar las buenas prácticas establecidas en la política de desarrollo de software y el Manual definido por la OTIC.	Documentación para los sistemas de información en desarrollo: • Solicitudes de cambio y análisis de riesgos. • Cronograma • Casos de uso • Requisitos Funcionales / No funcionales • Plan de pruebas funcionales y de seguridad. • Criterios de aceptación.	OTIC	01/02/2023	31/05/2023
Seguridad en las comunicaciones (T.5)	28	Pruebas e Implementación de mecanismos de control de acceso a la red.	Informe donde se evidencia las respectivas pruebas y funcionamiento.	OTIC	01/02/2023	31/12/2023
Desarrollo - Software (T.6)	29	Implementar el procedimiento o proceso para el acceso a datos de pruebas.	Documentación que evidencie las autorizaciones y el tipo de datos al que se va a tener acceso.	OTIC	01/02/2023	31/10/2023
Gestión de incidentes de seguridad de la información (T.7)	30	Definir protocolo de atención y respuesta a incidentes de seguridad de la información por tipo de incidente.	Protocolo o procedimiento documentado, incluyendo responsabilidades.	Oficial de seguridad de la información / OTIC	01/02/2023	31/05/2023

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA INICIO	FECHA FIN
	31	Documentar informes de incidentes de seguridad de la información clasificados como altos o muy altos.	Informes de incidentes que incluya la investigación, recolección de evidencia, lecciones aprendidas, contactos con autoridades, recomendaciones para actualizar la gestión de incidente, cuando corresponda, entre otros.	Oficial de seguridad de la información.	01/02/2023	31/05/2023

Fuente: Elaboración Propia

8. VERIFICACIÓN

La verificación del cumplimiento del plan se realizará a través del indicador “Ejecución del Plan de Seguridad y Privacidad de la Información” asociado al proceso de gestión tecnológica y de la información.

De igual forma, el Oficial de seguridad de la información en conjunto con la OTIC podrán realizar autoevaluaciones que consideren necesarias al Modelo de Seguridad y Privacidad de la Información implementado, por medio de la herramienta definida por el MinTIC, para verificar el estado actual y realizar los ajustes pertinentes al plan de acción o por medio de los instrumentos de planes de mejoramiento definidos en la Entidad.

9. APROBACIÓN

Elaboró	Sayra Paola Nova - Oficial de Seguridad de la Información Juan Sebastian Perdomo Mendez – Profesional Universitario OTIC
Revisó	Cesar Mauricio Beltran Lopez – Jefe Oficina TIC Mesa Técnica de Seguridad Digital – Acta de Reunión 23/01/2023
Aprobó	Comité Institucional de Gestión y Desempeño – Acta de Reunión 30 de enero de 2023

ALCALDÍA MAYOR
DE BOGOTÁ D.C.

UAESP
Unidad Administrativa Especial
de Servicios Públicos

BOGOTÁ