



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
Gerencia General	Código: DS-PSI-GG-001
	Versión: 1.0
	Clasificación de Información: Información de uso Público

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Aprobado por:	Firma de Aprobación:
Andrés Fernández - Gerente General	
	Fecha de Aprobación: 21 de abril de 2025

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
	Gerencia General	Código: DS-PSI-GG-001
		Versión: 1.0
		Clasificación de Información: Información de uso Público

ÍNDICE

1. Objetivo	3
1.1. General:	3
1.2. Específicos:	3
2. Alcance.....	4
3. Definiciones.....	4
4. Roles y Responsabilidades.....	6
5. Controles de Seguridad	7
6. Formación y Concientización	7
7. Monitoreo, Revisión y Difusión	8
8. Cumplimiento y Sanciones	8
9. Firmas de Responsabilidad	9
10. Control de Cambios.....	9

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
	Gerencia General	Código: DS-PSI-GG-001
		Versión: 1.0
		Clasificación de Información: Información de uso Público

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Objetivo

1.1. General:

- **Cumplimiento Normativo y Legal:** Asegurar que todas las actividades relacionadas con la gestión y seguridad de la información estén en conformidad con las legislación nacional aplicable.
- **Protección Integral de la Información:** Aplicar y mantener controles de seguridad avanzados para proteger la confidencialidad, integridad y disponibilidad de la información.
- **Fortalecimiento de la Cultura de Seguridad:** Fomentar la adopción de buenas prácticas de seguridad en toda la organización, promoviendo la responsabilidad y concienciación sobre la protección de la información.
- **Mejora Continua y Adaptabilidad:** Implementar un proceso de mejora continua que permita adaptar las políticas y controles a los cambios e innovaciones tecnológicas, amenazas emergentes y requisitos regulatorios.

1.2. Específicos:

- **Confidencialidad de la Información:** Implementar un sistema de control de acceso basado en roles y privilegios, que limite la exposición de información confidencial a personal no autorizado. Aplicar medidas de cifrado para proteger la información tanto en tránsito como en reposo, utilizando estándares recomendados.
- **Integridad de los Datos:** Utilizar mecanismos de verificación que aseguren que la información no ha sido alterada de manera no autorizada. Mantener un registro de auditoría que permita rastrear todas las modificaciones y accesos a la información crítica.
- **Disponibilidad de Sistemas y Datos:** Garantizar el acceso seguro y continuo a todos los servicios de Dentalsoft, a través de planes de contingencia, respaldos regulares y sistemas de recuperación ante desastres. Realizar simulacros de recuperación para asegurar la capacidad de respuesta en caso de incidentes, de igual manera evitando indisponibilidades del servicio.
- **Gestión de Riesgos:** Ejecutar evaluaciones de riesgos periódicas, identificando amenazas y vulnerabilidades que puedan impactar la seguridad de la información y tomar medidas preventivas. Mantener un registro actualizado de los riesgos identificados así como de las medidas de mitigación implementadas en anteriores evaluaciones.

Es esencial que posterior e inmediatamente a la identificación de una amenaza o vulnerabilidad, se ejecute un plan de corrección o mitigación en el área correspondiente

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
	Gerencia General	Código: DS-PSI-GG-001
		Versión: 1.0
		Clasificación de Información: Información de uso Público

para su aprobación, y ejecución, con el fin de minimizar los riesgos que amenazan a los activos de información que gestiona la organización.

- **Auditorías Internas y Monitoreo Continuo:** Realizar auditorías internas anuales para evaluar y monitorear el cumplimiento de la política y de los controles de seguridad. Implementar herramientas de monitoreo para detectar y responder a posibles amenazas en tiempo real.
- **Capacitación y Concienciación:** Ofrecer programas de formación continua sobre seguridad de la información a todos los empleados (internos y externos), enfatizando en la protección de datos y el uso seguro de las herramientas Dentalsoft y SAM. Realizar campañas de concienciación sobre temas como el phishing, ingeniería social y gestión segura de la información.

2. Alcance

2.1. Esta política se aplica a todos los sistemas, redes, dispositivos y recursos de Dentalsoft, así como a todos los empleados, colaboradores, contratistas, proveedores, prestadores de servicios y cualquier entidad que acceda, administre o interactúe con los sistemas de información, así como aquellos que proporcionen soporte o mantenimiento a los servicios críticos de la organización, abarcando también los datos y activos físicos o virtuales administrados en la operación.

3. Definiciones

3.1. Activo de Información: Recurso de Dentalsoft, como personas, instalaciones, procesos, archivos digitales, documentos, base de datos, intangibles e información en general, entre otros, que generen valor y que sean necesarios para la operación y el cumplimiento de sus objetivos.

3.2. Amenaza: Evento, acción o circunstancia que pueda explotar una vulnerabilidad y comprometer la confidencialidad, integridad o disponibilidad de los sistemas, datos o procesos de Dentalsoft. Las amenazas pueden ser de origen interno o externo y abarcan tanto factores intencionales, como ataques cibernéticos, como no intencionales, como desastres naturales o errores humanos.

3.3. Cifrado de Datos: Técnica de seguridad que transforma la información en un formato ilegible para quienes no tienen la clave de descryptación, protegiendo los datos tanto en tránsito como en reposo contra accesos no autorizados.

3.4. Confidencialidad: Propiedad de la información que garantiza que sólo las personas, sistemas o entidades autorizadas tengan acceso a los datos.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
	Gerencia General	Código: DS-PSI-GG-001
		Versión: 1.0
		Clasificación de Información: Información de uso Público

3.5. Disponibilidad: Característica de los sistemas de información que garantiza el acceso oportuno y confiable a los datos y servicios por parte de los usuarios autorizados cuando lo necesitan.

3.6. Impacto: Consecuencia o efecto de un incidente de seguridad sobre los sistemas, datos o procesos de Dentalsoft. El impacto puede manifestarse en términos de pérdida de confidencialidad, integridad o disponibilidad de la información, afectando la operación, reputación, cumplimiento normativo o los objetivos estratégicos de la organización.

3.7. Incidente de Seguridad: Suceso que compromete o tiene el potencial de comprometer la confidencialidad, integridad o disponibilidad de la información o de los sistemas de Dentalsoft. Ejemplos incluyen ataques de phishing, accesos no autorizados o fuga de información.

3.8. Integridad: Propiedad de la información asegura que la información es exacta y completa, protegiéndola contra modificaciones no autorizadas durante su almacenamiento o transmisión.

3.9. Phishing: Técnica de ingeniería social en la que un atacante se hace pasar por una entidad confiable para engañar a las personas y obtener información confidencial como contraseñas o datos bancarios.

3.10. Principio de Menor Privilegio: Enfoque de seguridad que otorga a los usuarios los permisos mínimos necesarios para cumplir con sus funciones, limitando su acceso a los recursos esenciales.

3.11. Probabilidad: Medida que indica la posibilidad de que ocurra un incidente de seguridad que pueda comprometer la confidencialidad, integridad o disponibilidad de los sistemas y datos de Dentalsoft. La probabilidad se evalúa en función de factores como la frecuencia de amenazas, vulnerabilidades presentes y la exposición a riesgos, y es utilizada en la gestión de riesgos para priorizar y tomar decisiones sobre los controles de seguridad necesarios.

3.12. Respaldo de Datos: Copia de seguridad de la información almacenada en medios externos o en la nube, que permite restaurar los datos en caso de pérdida o corrupción.

3.13. Riesgo: Posibilidad de que una amenaza explote una vulnerabilidad en los sistemas, procesos o datos de Dentalsoft, generando un impacto negativo sobre la confidencialidad, integridad o disponibilidad de la información.

3.14. Seguridad de la Información: Conjunto de procesos, metodologías, políticas, normativas, estándares, procedimientos, controles, software y otros elementos necesarios para mantener la confidencialidad, integridad y disponibilidad de la información.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
	Gerencia General	Código: DS-PSI-GG-001
		Versión: 1.0
		Clasificación de Información: Información de uso Público

3.15. Simulacro de Seguridad: Ejercicio planificado que simula incidentes de seguridad para evaluar la capacidad de respuesta y preparación del personal ante posibles amenazas.

3.16. Vulnerabilidad: Debilidad en los sistemas, redes o procesos que puede ser explotada por amenazas para comprometer la seguridad de la información.

4. Roles y Responsabilidades

4.1 Encargado de Seguridad de la Información: Responsable de la implementación, actualización, monitoreo y medición de las medidas de seguridad, así como de la coordinación de la respuesta ante incidentes de seguridad. El Encargado de Seguridad de la Información también es responsable de garantizar que todos los empleados y colaboradores estén debidamente capacitados en seguridad de la información.

4.2. Prestadores de Servicios: Todos los Prestadores de Servicios, Colaboradores y usuarios de los recursos de Dentalsoft deben cumplir con esta política y con los procedimientos de seguridad asociados a la empresa. Esto incluye las siguientes responsabilidades y deberes:

- a. Mantener debida reserva y bajo resguardo la información a la cual tuviese acceso autorizado.
- b. Abstenerse de acceder sin autorización escrita o indebidamente a terminales, archivos, documentación o datos de Dentalsoft y clientes.
- c. Abstenerse de instalar software o conectar equipos personales u otros elementos no autorizados, a la red de datos.
- d. Asegurar el resguardo de la confidencialidad, integridad y disponibilidad de la información de Dentalsoft y dar aviso al Encargado de Seguridad de la Información de cualquier situación o circunstancia que pueda afectar o poner en riesgo la información o los sistemas de procesamiento de información.
- e. Abstenerse de realizar actos contrarios a la propiedad física e intelectual de Dentalsoft, particularmente a la incluida en entornos digitales, tales como diseños de procesos, modelos de bases de datos y aplicaciones de negocios; así como también de vulnerar contratos de licenciamiento de software y similares, suscritos por Dentalsoft con sus proveedores de tecnologías de información.
- f. Utilizar los recursos informáticos para desempeñar sólo las funciones que le fueron asignadas.
- g. Mantener en adecuadas condiciones los elementos de tecnología de Información entregados para el desempeño de su trabajo.
- h. Conocer y cumplir las normas y procedimientos asociadas al uso de los recursos tecnológicos y activos de información a los que se le otorgue acceso, como por ejemplo, aquellas asociadas al uso de contraseñas, del correo electrónico y del acceso a redes públicas como Internet.

 DentalSoft	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
	Gerencia General	Código: DS-PSI-GG-001
		Versión: 1.0
		Clasificación de Información: Información de uso Público

- i. Colaborar con los controles, monitoreos y procesos de auditoría orientados a verificar el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los recursos de información, tanto lógicos como físicos.

4.3. Proveedores y Terceros: Los proveedores que manejan o acceden a la información de Dentalsoft deben cumplir con los mismos estándares de mecanismos y controles de seguridad definidos por la empresa, así como leyes vigentes en el país. Se requerirá la firma de acuerdos de confidencialidad y no divulgación de la información entre partes y el cumplimiento de las normativas aplicables con la finalidad de proteger a la empresa de los riesgos asociados así como la protección a los activos de información involucrados en el ciclo de vida del servicio a prestar. Asimismo, dentro del contrato de servicios se indicará el derecho que tiene Dentalsoft de solicitar al proveedor evidencias que avalen sus estándares y niveles adecuados en aspectos de seguridad.

5. Controles de Seguridad

5.1. Control de Acceso: El acceso a los sistemas de información de Dentalsoft estará limitado a usuarios autorizados según su rol y necesidad de acceso. Se implementarán mecanismos como autenticación multifactor (MFA) y controles de acceso basados en roles para proteger la información crítica.

5.2. Cifrado de Datos: Se utilizarán técnicas criptográficas avanzadas para proteger la información tanto en tránsito como en reposo.

5.3. Respaldo y Recuperación de Datos: Dentalsoft implementará políticas de respaldo regular y procedimientos de recuperación ante desastres para asegurar que la información pueda ser restaurada rápidamente en caso de pérdida o corrupción de datos, garantizando la continuidad de los servicios y la integridad de los datos críticos, minimizando tiempos de inactividad y riesgos de pérdida de información.

5.4. Gestión de Incidentes de Seguridad: Dentalsoft contará con un plan de respuesta a incidentes de seguridad que incluirá la detección, notificación y mitigación de cualquier incidente que pueda comprometer la seguridad de la información. Se establecerán líneas de comunicación claras y canales específicos para asegurar la notificación inmediata de incidentes.

6. Formación y Concientización

6.1. La organización promoverá una cultura de seguridad de la información a través de programas de formación y concienciación dirigidos a todo el personal y colaboradores. Esta iniciativa tiene como objetivo asegurar que todos los usuarios conozcan y comprendan los

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
	Gerencia General	Código: DS-PSI-GG-001
		Versión: 1.0
		Clasificación de Información: Información de uso Público

riesgos asociados al uso de la información y las buenas prácticas necesarias para protegerla, adaptándose a sus funciones y responsabilidades.

6.2. Se impartirá formación básica a todo el personal al momento de su incorporación, así como sesiones periódicas de actualización. Además, se desarrollarán acciones específicas para colectivos con funciones críticas, como administradores de sistemas o responsables de tratamiento de datos. Las campañas de concienciación se reforzarán mediante comunicados internos, materiales visuales y actividades prácticas.

6.3. El Encargado de seguridad de la Información mantendrá registros de las actividades formativas realizadas y evaluará su eficacia periódicamente, incorporando mejoras continuas. Estas acciones forman parte del compromiso de la organización con la protección de la información, el cumplimiento normativo y la prevención de incidentes de seguridad.

7. Monitoreo, Revisión y Difusión

7.1. La organización establecerá mecanismos de monitoreo y revisión continua de la Política de Seguridad de la Información y de las medidas asociadas, con el fin de garantizar su eficacia y adecuación frente a cambios tecnológicos, normativos y organizativos. Este proceso incluirá auditorías internas, revisión de incidentes y evaluaciones periódicas.

7.2. La política y sus actualizaciones serán comunicadas de forma clara y accesible a todo el personal mediante los canales corporativos establecidos, asegurando su adecuada comprensión y aplicación. La difusión se realizará **al menos una vez al año** o siempre que se introduzcan cambios relevantes en los lineamientos de seguridad.

7.3. La responsabilidad de supervisar el cumplimiento de este proceso recaerá en el Encargado de Seguridad de la Información, quien coordinará con las distintas áreas los ajustes necesarios para mantener un entorno seguro y alineado con los objetivos estratégicos de la organización.

8. Cumplimiento y Sanciones

8.1. El cumplimiento de la presente política es obligatorio para todo el personal de la organización, así como para terceros que tengan acceso a los sistemas o a la información corporativa. Se considerará infracción cualquier acción u omisión que vulnere los principios y normas establecidos, especialmente si compromete la confidencialidad, integridad o disponibilidad de la información.

8.2. En caso de incumplimiento, se podrán aplicar medidas correctivas y sanciones conforme a la normativa laboral, contractual o disciplinaria vigente, sin perjuicio de las responsabilidades legales que pudieran derivarse. Estas sanciones serán proporcionales a la gravedad de la falta y evaluadas por las instancias competentes.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
	Gerencia General	Código: DS-PSI-GG-001
		Versión: 1.0
		Clasificación de Información: Información de uso Público

8.3. La organización promueve un entorno de responsabilidad y cumplimiento, apoyado en la existencia de canales de consulta y denuncia, que permitan comunicar posibles incumplimientos de forma confidencial y segura.

9. Firmas de Responsabilidad

Elaborado por:	Firma
Nombre: Rodrigo Hume Cargo: Encargado de Seguridad de la Información	

Revisado por:	Firma
Nombre: Dagoberto Fernández Cargo: Director	

Aprobado por:	Firma
Nombre: Andrés Fernández Cargo: Gerente General	

10. Control de Cambios

VERSIÓN	DETALLE	ELABORADO POR:	FECHA APROBACIÓN	APROBADO POR:
1.0	Versión Inicial	Rodrigo Hume	21-04-2025	Andrés Fernández