

	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-007
	POLITICA ESPECIFICA DE SEGURIDAD OPERACIONAL	Versión:	3.0
DACTA SAC	DOCUMENTO CONTROLADO	Vigente desde:	22/02/2024
		Página:	1 de 7

Política Específica de Seguridad Operacional

	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-007
	POLITICA ESPECIFICA DE SEGURIDAD OPERACIONAL	Versión:	3.0
DACTA SAC	DOCUMENTO CONTROLADO	Vigente desde:	22/02/2024
		Página:	2 de 7

ÍNDICE

1. OBJETIVO, ALCANCE Y USUARIOS	3
2. DOCUMENTOS DE REFERENCIA	3
3. POLÍTICA ESPECÍFICA	3
3.1. PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES DOCUMENTADAS....	3
3.2. GESTIÓN DEL CAMBIO.....	4
3.3. GESTIÓN DE LA CAPACIDAD.....	4
3.4. SEPARACIÓN DE ENTORNOS DE DESARROLLO, OPERACIÓN Y PRUEBAS	4
3.5. PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y CÓDIGO MÓVIL	5
3.6. BACKUP.....	5
3.7. GESTIÓN TÉCNICA DE VULNERABILIDADES	5
3.8. CONSIDERACIONES PARA AUDITAR SISTEMAS DE INFORMACIÓN	6
4. REGISTROS	7
5. CONTROL DE CAMBIOS.....	7

	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-007
	POLITICA ESPECIFICA DE SEGURIDAD OPERACIONAL	Versión:	3.0
DACTA SAC	DOCUMENTO CONTROLADO	Vigente desde:	22/02/2024
		Página:	3 de 7

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es establecer las directrices para la aplicación de controles de seguridad para garantizar las operaciones de DACTA.

Este documento se aplica a todo el alcance del Sistema Integrado de Gestión (SIG); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SIG.

Los usuarios de este documento son todos los colaboradores de DACTA.

2. DOCUMENTOS DE REFERENCIA

- NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información, cláusulas 5.24, 5.25, 5.26, 5.27, 5.28, 5.29, 5.30, 8.6, 8.32, 8.4, 8.25, 8.29, 8.30, 8.31.

3. POLÍTICA ESPECÍFICA

La Seguridad Operacional es una cuestión central para DACTA, por eso nos comprometemos a gestionar los procesos, optimizando los recursos para lograr el más alto desempeño de Seguridad Operacional.

- Dar la máxima prioridad a la Seguridad Operacional en la provisión de nuestros servicios, evaluando los riesgos y determinando los niveles de seguridad aceptables.
- Investigar toda incidencia que pueda repercutir en la Seguridad Operacional, identificando sus causas raíces para poder tomar acciones que eviten su repetición.
- Promover el reporte de eventos que afecten a la Seguridad Operacional a través del establecimiento de una Cultura Justa; salvo casos de flagrante negligencia, nadie será sancionado como consecuencia de un reporte.
- Monitorear la efectividad de nuestros procesos, con orientación a la Mejora Continua.
- Establecer una cultura de gestión planificada de las contingencias para prevenir cualquier deterioro en las operaciones.
- Apoyar la Seguridad Operacional con recursos humanos y financieros.
- Asignar responsabilidades y obligaciones a todas las gerencias, con respecto a la priorización de la Seguridad Operacional en el marco de sus actividades.

Cumplir con la normativa.


- Capacitar al personal en materia de Seguridad Operacional.
- Definir objetivos de Seguridad Operacional y medir nuestro cumplimiento.
- Revisar periódicamente el sistema, incluyendo nuestras políticas y objetivos, para impulsar la mejora continua.

Esta política debe ser comprendida, respetada e implementada por todo el personal de DACTA.

3.1. PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES DOCUMENTADAS

Toda nuestra organización se compromete a contar con procedimientos claros y precisos a fin de integrar y facilitar las operaciones en todos los niveles:

- Instrucciones documentadas para la instalación y configuración de las diferentes aplicaciones en los servidores de DACTA SAC o de sus clientes, ya sean estas desarrolladas por DACTA o por terceras empresas.
- Instrucciones documentadas para la realización de backups.

	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-007
	POLITICA ESPECIFICA DE SEGURIDAD OPERACIONAL	Versión:	3.0
DACTA SAC	DOCUMENTO CONTROLADO	Vigente desde:	22/02/2024
		Página:	4 de 7

- Instrucciones para el procesamiento de incidentes que pudieran surgir durante la ejecución del trabajo.
- Contactos de soporte y escalado, incluyendo los contactos de soporte externo, en el caso de experimentar dificultades técnicas u operacionales.
- Tratamiento seguro de los medios ante salidas de información crítica o sensible.
- Pasos de reinicio y recuperación a utilizar en el caso de que el sistema falle.
- La gestión de revisión y monitoreo de logs de los sistemas de información críticos.
- Las actualizaciones de versiones de sistemas operativos en los servidores

3.2. GESTIÓN DEL CAMBIO


- Se debe motivar y respaldar toda iniciativa de cambio que encaje dentro del proceso de mejora continua al interior de la organización.
- Se deben identificar las necesidades de cambios, valorando los impactos potenciales, incluyendo impactos en la seguridad de la información. Toda propuesta de cambio, que involucre una inversión, debe cumplir un objetivo, estar sustentada y acompañada del o de los indicadores que permitirán medir la eficacia del cambio.
- Los cambios a ejecutar, previamente se deben aprobar por las instancias respectivas dependiendo de la magnitud de los cambios.
- Los cambios ejecutados deben evacuar registros de información necesarios para permitir el cálculo del indicador que permita medir la mejora lograda.
- Los cambios que deban realizarse en atención a una no conformidad deben tener prioridad en los planes de actividades dentro de toda la organización.
- Se comunicarán el detalle de los cambios a todas las partes interesadas afectadas.

3.3. GESTIÓN DE LA CAPACIDAD

- Se debe monitorear el uso de los recursos, de forma que se puedan hacer proyecciones sobre los requisitos de capacidad futuros, asegurando así el rendimiento requerido de los sistemas.
- Se realizan las siguientes actividades para la gestión de la capacidad:
 - Monitorización del espacio para almacenamiento de información.
 - Eliminación de aplicaciones, sistemas, bases de datos y entornos no justificados en DACTA.
 - Análisis de la demanda actual y futura.
 - Optimización de procesos en todas las áreas.
 - Optimización de la lógica de las aplicaciones y de las consultas a la Base de Datos.
 - Denegación o restricción de recursos / ancho de banda a posibles servicios con un alto consumo que no son críticos para la organización.
 - La gestión de la capacidad podrá ser lograda mediante la gestión de la demanda de capacidad en DACTA.

3.4. SEPARACIÓN DE ENTORNOS DE DESARROLLO, PRUEBAS, BETA Y PRODUCCION

- Se debe definir y documentar las reglas para transferir el software del entorno de desarrollo, pruebas, beta y producción.
- Se debe documentar el software desarrollado, probado y listo para instalarse en producción. El equipo de Desarrollo definirá los aspectos técnicos a considerar en dicha documentación.
- Los cambios en las aplicaciones deben testearse en un entorno de pruebas, antes de ser instalados en entornos de producción.
- Salvo en circunstancias excepcionales, formalmente autorizadas, las pruebas no deberán hacerse en entornos de producción.

	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-007
	POLITICA ESPECIFICA DE SEGURIDAD OPERACIONAL	Versión:	3.0
DACTA SAC	DOCUMENTO CONTROLADO	Vigente desde:	22/02/2024
		Página:	5 de 7

- Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no serán accesibles como parte de los entornos de producción.
- Los usuarios deben utilizar diferentes perfiles para los sistemas de prueba y para los entornos de producción; por ejemplo, el analista, desarrollador, QA, etc.
- Los datos sensibles no deben copiarse en el entorno de pruebas, a no ser que se implementen controles de seguridad equivalentes a los implantados en entornos de producción.

3.5. PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y CÓDIGO MÓVIL

- DACTA cuenta con un sistema de seguridad perimetral redundante que incluye firewall y antivirus integrado para hacer frente a cualquier tipo de malware que pudiera presentarse por nuestros enlaces de Internet.
- En el caso de las computadoras o servidores con sistema operativo Windows es obligatorio la activación de la Seguridad de Windows y de un agente de antivirus en todos los equipos.

3.6. BACKUP

- DACTA cuenta con un plan de copia de seguridad para disponer de la información en caso de falle el servidor de base de datos.
- Se establece la periodicidad, así como el tipo de copia en función de las necesidades de DACTA.
- Se acota y completa los registros de las copias de seguridad y existirán procedimientos de recuperación.
- Se ejecuta las pruebas sobre los planes de recuperación de información y los sistemas, de acuerdo a los requisitos de DACTA.
- Las copias de seguridad se almacenan en un sitio externo respecto de la ubicación habitual de los sistemas y la información.

3.7. GESTIÓN TÉCNICA DE VULNERABILIDADES

- Se gestionan las vulnerabilidades, realizando análisis de vulnerabilidades según la criticidad del sistema, con una periodicidad mínima anual.
- Los problemas encontrados se analizan y se aplican las medidas correctoras en función del riesgo de la vulnerabilidad encontrada.

3.8. SINCRONIZACION DE RELOJES


Se han definido las políticas y directivas necesarias para que los equipos informáticos sincronicen sus relojes con el servidor de la organización a través del Directorio activo, a fin de, entre otros aspectos, asegurar la integridad y la eficacia de los eventos y registros de los sistemas.

Por ello, queda prohibida la instalación de software en los equipos por parte del propio personal de DACTA.

Adicionalmente, los equipos servidores se encuentran sincronizados con sistemas externos de sincronización horaria a fin de disponer una trazabilidad con una hora oficial. A este efecto se utiliza el servidor externo de Windows (time.windows.com).

3.9. INSTALACION DE SOFTWARE

El Coordinador de TI o la persona que designe y cuente con derechos de administrador, será el/ los único/s autorizados para instalar un software o aplicación en los equipos de DACTA S.A.C.

	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-007
	POLITICA ESPECIFICA DE SEGURIDAD OPERACIONAL	Versión:	3.0
DACTA SAC	DOCUMENTO CONTROLADO	Vigente desde:	22/02/2024
		Página:	6 de 7

Adicionalmente, como parte de la implementación de software o aplicaciones en DACTA, previamente a su instalación, se deberá realizar las pruebas piloto previo a su despliegue en toda la organización. Esto queda a cargo del Coordinador de TI quien designa al equipo requerido para las pruebas y su implementación.

3.10. SEGURIDAD EN LOS SERVICIOS DE RED

Para la seguridad en los servicios de red se cuenta con un servicio de seguridad perimetral, el cual es brindado por un proveedor de servicios que tiene a su cargo el brindar las características de seguridad requeridas por DACTA.

El seguimiento de estos niveles de servicios se realiza por parte del OSI a través F-E-SIG-214 Seguimiento a niveles de servicio de proveedores.

3.11. CONSIDERACIONES PARA AUDITAR SISTEMAS DE INFORMACIÓN

Los requisitos de auditoría y actividades involucradas en la explotación de los sistemas operacionales son planificados con el objetivo de minimizar las interrupciones en la operación de los procesos de DACTA.






En caso de no cumplir con la presente Política Específica de Seguridad Operacional, los lineamientos de seguridad de la información u otros directivas o procedimientos de seguridad de la información, se reportará el evento al Oficial de Seguridad de la Información para que tome conocimiento y disponga las acciones correspondientes, de considerarlo necesario. De esta forma, tomará las medidas disciplinarias necesarias, las cuales están sujetas al Código de ética y conducta de la DACTA.

DACTA	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-007
	POLITICA ESPECIFICA DE SEGURIDAD OPERACIONAL	Versión:	3.0
DACTA SAC	DOCUMENTO CONTROLADO	Vigente desde:	22/02/2024
		Página:	7 de 7

4. REGISTROS

Código	Nombre de Registro	Responsable del Control	Tiempo de Conservación
F-E-SIG-214	Seguimiento a niveles de servicio de proveedores	OSI	3 años

5. CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Elaborado por	Revisado por	Aprobado por
1	30/06/2021	Emisión	OSI	Comité SIG	Gerente General
2	08/09/2021	Actualización	OSI	Comité SIG	Gerente General
3	22/02/2023	Actualización	OSI	Comité SIG	Gerente General
3	22/02/2024	Revisión	OSI	Comité SIG	Gerente General
Firmas de la versión vigente					
			S. Rafaile	S. Rafaile	
					
			A. Morales	A. Morales	
Identificación de las modificaciones					
Versión	Descripción de cambios				
2	Se incorpora lo relacionado a la sincronización de relojes y a la política de instalación de software.				
3	Se actualizó el documento con el nuevo logo de DACTA. Se actualiza el requisito normativo según nueva versión ISO 27001:2022.				