
	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-002
	POLITICA ESPECIFICA DE PANTALLA Y ESCRITORIO LIMPIO	Versión:	4.0
		Vigente desde:	18/11/2024
DACTA SAC	DOCUMENTO CONTROLADO	Página:	1 de 6

## Política Específica de Pantalla y Escritorio Limpio

### RESTRINGIDO

Este documento una vez impreso se convertirá en una copia no controlada, a menos que cuente con un sello de "Copia Controlada", antes de su aplicación, consulte su vigencia con el Comité del SIG.


	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-002
	POLITICA ESPECIFICA DE PANTALLA Y ESCRITORIO LIMPIO	Versión:	4.0
		Vigente desde:	18/11/2024
DACTA SAC	DOCUMENTO CONTROLADO	Página:	2 de 6

## ÍNDICE

1. OBJETIVO, ALCANCE Y USUARIOS .....	3
2. DOCUMENTOS DE REFERENCIA .....	3
3. POLÍTICA ESPECÍFICA .....	3
5. REGISTROS .....	5
6. CONTROL DE CAMBIOS.....	5

### RESTRINGIDO

Este documento una vez impreso se convertirá en una copia no controlada, a menos que cuente con un sello de "Copia Controlada", antes de su aplicación, consulte su vigencia con el Comité del SIG.

	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-002
	POLITICA ESPECIFICA DE PANTALLA Y ESCRITORIO LIMPIO	Versión:	4.0
DACTA SAC	DOCUMENTO CONTROLADO	Vigente desde:	18/11/2024
		Página:	3 de 6

## 1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir reglas para evitar el acceso no autorizado a la información en los puestos de trabajo, como también a las instalaciones y a los equipos compartidos. Así mismo mantener el orden y la limpieza de los puestos de trabajo.

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, clausula 7.7.


## 3. POLÍTICA ESPECÍFICA

Se adopta una política de escritorio limpio, para proteger documentos en papel y dispositivos de almacenamiento removibles y de pantalla limpia, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo en las instalaciones de DACTA.

Todo colaborador de DACTA o tercero para el desempeño de sus funciones, está obligado a cumplir las siguientes políticas:

- Toda información generada, producida o transformada dentro de las instalaciones de DACTA, es de propiedad intelectual de ésta y está calificada como confidencial. De la misma manera sucede con cualquier información generada o transformada por cualquier colaborador, en el medio que sea, y si su generación o transformación se realiza como parte de sus labores y responsabilidades adquiridas contractualmente con DACTA. Por ende, está prohibido de copiarla para sí, compartirla con terceras personas, copiarla o publicarla en servidores públicos.
- Guardar bajo llave en gabinetes y/u otro tipo de mobiliario seguro cuando corresponda, todo documento en papel y/o en medios de almacenamiento óptico y/o magnético cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- DACTA asignará el mobiliario necesario para la custodia de la información mencionada en el párrafo anterior. Los usuarios de gabinete(s) con llave serán responsables de la custodia de la(s) llave(s) asignada(s).
- En caso de que los repositorios, donde se guarde la documentación, cualquiera sea el medio que la contenga, se encuentren dentro de las instalaciones de DACTA, Recursos Humanos custodiará copias de las llaves físicas de dichos repositorios.
- Desconectar de la red (Eléctrica, LAN, WAN) todo equipo que no se encuentre en uso.
- Bloquear manualmente la sesión del computador, al momento de ausentarse del puesto de trabajo cuando asista a una reunión interna, uso de servicios higiénicos, salidas breves de las instalaciones. En el caso de reuniones prolongadas fuera de las instalaciones deberá cerrar sesión y apagar los equipos con los que se encuentre trabajando.
- Queda prohibido, para todo el personal, traer o ingresar a los ambientes de DACTA dispositivos de almacenamiento externos USB o discos externos de su propiedad. Los únicos dispositivos permitidos serán los de propiedad de DACTA y deberá estar justificado su uso y controlado la tenencia de éstos.

**RESTRINGIDO**

	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-002
	POLITICA ESPECIFICA DE PANTALLA Y ESCRITORIO LIMPIO	Versión:	4.0
DACTA SAC	DOCUMENTO CONTROLADO	Vigente desde:	18/11/2024
		Página:	4 de 6

- Reportar al Coordinador de TI y/o al Oficial de seguridad la tenencia o presencia de cualquier dispositivo de almacenamiento externos USB dentro de las instalaciones.
- Queda prohibido la conexión de cualquier dispositivo electrónico (Memoria USB, Teléfono celular, discos externos) a las computadoras que utiliza el personal dentro de las instalaciones de DACTA. El Coordinador de TI velará que ningún colaborador conecte a su equipo de cómputo los dispositivos externos mencionados pudiendo decomisar éstos si amerita el caso. En cualquier caso, de darse este hecho, el Oficial de seguridad está obligado a reportar a la Gerencia respectiva la queja correspondiente por el incumplimiento de esta política.
- Únicamente personal de Soporte de TI estará autorizado a utilizar dispositivos de almacenamiento USB dentro de las instalaciones de DACTA en los siguientes casos:
  - Dentro del Data Center, para permitir el respaldo en línea de las bases de datos de servidores de producción. Los dispositivos de almacenamiento externo deben estar conectados permanentemente a los servidores y configurados correctamente.
  - En el espacio donde se realice el mantenimiento de los equipos, para realizar la instalación de software base en computadoras y servidores.
- El uso de estos dispositivos por parte de Soporte de TI será estrictamente controlado por el Coordinador de TI.
- El Coordinador de TI es el responsable de implementar los controles necesarios para evitar que cualquier usuario pueda hacer uso, libremente, de los puertos USB de la computadora que le haya sido asignada.
- El colaborador se asegurará de no reutilizar hojas de papel con información confidencial o datos personales como: (CV, información financiera, certificaciones laborales, arquitectura, ofertas comerciales, información de clientes, etc.)
- Ningún colaborador podrá exponer información confidencial, de DACTA. en lugares públicos sin previa autorización escrita de la Gerencia General.
- Los colaboradores que hagan uso de pizarras para escribir sobre ellas, deberán borrarlas luego de la culminación de la reunión o evento que conllevó a su uso.
- Cada colaborador deberá mantener el escritorio de computadora que le haya sido asignada; libre de archivos que contengan información relevante sobre el trabajo que realiza.
- El carácter de confidencial o clasificada que se pueda dar a cierta información lo deberán saber únicamente las personas involucradas directamente en el manejo de dicha información. El Gerente del área, de ser el caso, solicitará asesoría al Coordinador de TI y al Oficial de seguridad para conocer la mejor forma de proteger dicha información confidencial.
- Cada colaborador es responsable de la confidencialidad de las contraseñas que utiliza, así como por el cambio de estas.
- Cada colaborador es absolutamente responsable de la información que se tenga almacenada en el disco duro de la computadora que le sea asignada para su uso diario.
- Queda totalmente prohibido almacenar en el disco de la computadora que tenga asignada: Información personal o información de propiedad de DACTA y que no sea de su competencia o no se le haya autorizado formalmente a acceder. Del mismo modo queda prohibido guardar información de valor que se genere como parte de sus funciones, en el disco de la computadora asignada. Toda información valiosa debe ser integrada o almacenada en los servidores de DACTA destinada para estos fines.
- El bloqueo de las pantallas debe activarse automáticamente y debe ser controlada por el servidor controlador de dominio. Debe definirse un tiempo límite, no mayor a 30 minutos, de tal manera que si la PC del usuario no reciba una interacción la pantalla debe bloquearse en forma automática.

### RESTRINGIDO

<b>DACTA</b>	SISTEMA INTEGRADO DE GESTIÓN	<b>Código</b>	<b>L-E-SIG-002</b>
	<b>POLITICA ESPECIFICA DE PANTALLA Y ESCRITORIO LIMPIO</b>	<b>Versión:</b>	<b>4.0</b>
DACTA SAC	<b>DOCUMENTO CONTROLADO</b>	<b>Vigente desde:</b>	<b>18/11/2024</b>
		<b>Página:</b>	<b>5 de 6</b>

En caso de no cumplir con la presente Política Específica de Pantalla y Escritorio Limpio, 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 (OSI) para que tome conocimiento y disponga las acciones correspondientes, de considerarlo necesario. De esta forma, la autoridad competente de DACTA, tomará las medidas disciplinarias necesarias, las cuales están sujetas a la normativa vigente de DACTA.




#### 4. AUDITORÍA

- Los Dueños de proceso y el Oficial de Seguridad de la Información son los responsables de hacer cumplir estas políticas.
- El Oficial de Seguridad de la Información de DACTA se encargará de verificar el cumplimiento de estas políticas, de manera obligatoria, en forma trimestral, efectuando auditorías a todos los equipos de la organización.
- El Oficial de Seguridad de la Información de DACTA podrá verificar el cumplimiento de esta política de manera inopinada o a solicitud de la gerencia o jefatura que lo requiera.

#### 5. REGISTROS

<b>Código</b>	<b>Nombre de Registro</b>	<b>Responsable del Control</b>	<b>Tiempo de Conservación</b>
F-E-SIG-001	Registro de revisión de pantallas y escritorios limpios	Oficial de Seguridad de la Información	03 meses



#### 6. CONTROL DE CAMBIOS

<b>Versión</b>	<b>Fecha</b>	<b>Descripción</b>	<b>Elaborado por</b>	<b>Revisado por</b>	<b>Aprobado por</b>
1.0	30/06/2021	Emisión	OSI	Comité SIG	Gerente General
2.0	03/09/2021	Actualización	OSI	Comité SIG	Gerente General
3.0	22/02/2023	Actualización	OSI	Comité SIG	Gerente General
3.0	22/02/2024	Revisión	OSI	Comité SIG	Gerente General
4.0	18/11/2024	Actualización	OSI	Comité SIG	Gerente General
<b>Firmas de la versión vigente</b>					
			S. Rafaile	S. Rafaile	

**RESTRINGIDO**

Este documento una vez impreso se convertirá en una copia no controlada, a menos que cuente con un sello de "Copia Controlada", antes de su aplicación, consulte su vigencia con el Comité del SIG.

<b>DACTA</b>	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-002
	POLITICA ESPECIFICA DE PANTALLA Y ESCRITORIO LIMPIO	Versión:	4.0
		Vigente desde:	18/11/2024
DACTA SAC	DOCUMENTO CONTROLADO	Página:	6 de 6

			
	A. Morales	A. Morales	G. Rafaile
Identificación de las modificaciones			
Versión	Descripción de cambios		
2	<ul style="list-style-type: none"> <li>La información sensible o crítica debe ser protegida mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso. Recursos humanos custodiará copias de las llaves físicas de los gabinetes.</li> <li>Los usuarios de gabinetes con llave serán responsables de la custodia de sus llaves asignadas.</li> <li>Desconectar de la red (Eléctrica, LAN, WAN) todo equipo que no se encuentre en uso.</li> <li>El uso de estos dispositivos por parte de Soporte de TI será estrictamente controlado por el Coordinador de TI.</li> <li>Los colaboradores que hagan uso de pizarras para escribir sobre ellas, deberán borrarlas luego de la culminación de la reunión o evento que conllevó a su uso.</li> <li>Únicamente personal de Soporte de TI estará autorizado a utilizar dispositivos de almacenamiento USB dentro de las instalaciones de DACTA en los siguientes casos: <ul style="list-style-type: none"> <li>Dentro del Data Center, para permitir el respaldo en línea de las bases de datos de servidores de producción. Los dispositivos de almacenamiento externo deben estar conectados permanentemente a los servidores y configurados correctamente.</li> <li>En el espacio donde se realice el mantenimiento de los equipos, para realizar la instalación de software base en computadoras y servidores.</li> </ul> </li> </ul>		
3	<ul style="list-style-type: none"> <li>Se actualizó el documento con el nuevo logo de DACTA.</li> <li>Se actualiza el requisito normativo según nueva versión ISO 27001:2022.</li> </ul>		
4	<ul style="list-style-type: none"> <li>Se añadió un acápite sobre el bloque automático de las pantallas.</li> </ul>		

### RESTRINGIDO

Este documento una vez impreso se convertirá en una copia no controlada, a menos que cuente con un sello de "Copia Controlada", antes de su aplicación, consulte su vigencia con el Comité del SIG.