



**POLÍTICA DE SEGURIDAD FÍSICA Y
DEL AMBIENTE**

DESYSWEB

Lima - Perú



POLÍTICA	Código:	SGSI-POL-07
	Versión:	1.0
SEGURIDAD FÍSICA Y DEL AMBIENTE	Aprobado	Oswaldo Veas
	Fecha Aprob.:	20 abril 2020
	Página	2 de 8

CONTENIDO

1. OBJETIVO	3
2. ALCANCE	3
3. DEFINICIONES	3
4. POLÍTICA	3
4.1. Áreas Seguras	3
4.1.1. Perímetro de Seguridad Física	3
4.1.2. Controles de Acceso Físico	3
4.1.3. Seguridad de Oficinas, Despachos e Instalaciones	4
4.1.4. Protección Contra Amenazas Externas y del Ambiente	4
4.1.5. Trabajo en las Áreas Seguras	4
4.1.6. Áreas de Entrega y de Carga	4
4.2. Equipamiento	5
4.2.1. Ubicación y Protección del Equipamiento	5
4.2.2. Servicios de Apoyo	5
4.2.3. Seguridad en el Cableado	6
4.2.4. Mantenimiento del Equipamiento	6
4.2.5. Retiro de los Activos	6
4.2.6. Seguridad del Equipamiento y de los Activos Fuera de las Instalaciones de la Organización	7
4.2.7. Seguridad en la Reutilización o Disposición Final de Equipos	7
4.2.8. Equipo Desatendido por el Usuario	7
4.2.9. Política de Escritorio y Pantalla Limpios	7

	POLÍTICA	Código:	SGSI-POL-07
		Versión:	1.0
	SEGURIDAD FÍSICA Y DEL AMBIENTE	Aprobado	Oswaldo Veas
		Fecha Aprob.:	20 abril 2020
		Página	3 de 8

1. OBJETIVO

Evitar accesos físicos no autorizados, daños e interferencias contra la información de Desysweb S.A.C. y las instalaciones de procesamiento de información.

2. ALCANCE

Aplica a todo el personal que labora en Desysweb S.A.C.

3. DEFINICIONES

Están detalladas en la Norma Internacional ISO/IEC 27000:2016 "Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Información general y vocabulario".

4. POLÍTICA


4.1. Áreas Seguras

4.1.1. Perímetro de Seguridad Física

- Están definidos los perímetros de seguridad para el ingreso a las instalaciones.
- Cuenta con área de recepción atendida por personal de Desysweb S.A.C. y el acceso es restringido solo para personal autorizado.

4.1.2. Controles de Acceso Físico

- Proteger las áreas de seguridad para asegurar que solo se permite el ingreso de personal autorizado.
- Registra los nombres, la fecha, hora de entrada y salida de visitantes, este registro debe estar actualizado.
- El acceso a áreas donde se procesa o almacena información es restringido solo para personal autorizado.

	POLÍTICA	Código:	SGSI-POL-07
		Versión:	1.0
	SEGURIDAD FÍSICA Y DEL AMBIENTE	Aprobado	Oswaldo Veas
		Fecha Aprob.:	20 abril 2020
		Página	4 de 8

- Los derechos de acceso a áreas seguras son revisados actualizados y revocados cuando es necesario.

4.1.3. Seguridad de Oficinas, Despachos e Instalaciones

- Restringe el acceso al personal ajeno a Desysweb S.A.C. a la información de directorios y libros de teléfonos internos, que identifican ubicaciones de instalaciones sensibles de procesamiento de la información.
- Se debe evitar que la información confidencial o las actividades confidenciales sean visibles y/o escuchadas desde el exterior.

4.1.4. Protección Contra Amenazas Externas y del Ambiente

- Cuenta con asesoramiento especializado sobre cómo evitar los daños causados por incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o artificiales.

4.1.5. Trabajo en las Áreas Seguras

- Todo trabajo que se realice en áreas seguras es supervisado, para evitar actividades maliciosas.
- No está permitido la presencia de equipos de fotografía, video, audio u otras formas de registro, salvo autorización expresa.

4.1.6. Áreas de Entrega y de Carga

- El acceso a las áreas de entrega y de carga están restringidos solo al personal autorizado.
- El personal de entrega no tiene acceso a otra zona del local.
- Todo material entrante y saliente es inspeccionado, examinado y registrado.

	POLÍTICA	Código:	SGSI-POL-07
		Versión:	1.0
	SEGURIDAD FÍSICA Y DEL AMBIENTE	Aprobado	Oswaldo Veas
		Fecha Aprob.:	20 abril 2020
		Página	5 de 8

4.2. Equipamiento

4.2.1. Ubicación y Protección del Equipamiento

- Los equipos de Desysweb S.AC. deben ubicarse o protegerse para reducir los riesgos ocasionados por amenazas, peligros ambientales y oportunidades de acceso no autorizado, considerar:
 - Todo equipo debe situarse minimizando el acceso innecesario a las áreas de trabajo.
 - Las instalaciones de procesamiento de la información que manejan datos sensibles deben colocarse cuidadosamente, asegurarse y aislar los equipos que requieran protección para reducir el riesgo de que la información sea vista por personas no autorizadas.
 - Implementa controles para reducir el riesgo de amenazas físicas potenciales.
 - Establece pautas para comer, beber y fumar en proximidad de las instalaciones de procesamiento de la información.
 - Supervisa las condiciones ambientales, tales como temperatura y humedad, para verificar que las mismas no afecten negativamente el funcionamiento de las instalaciones de procesamiento de la información.

4.2.2. Servicios de Apoyo

- Los servicios de apoyo tales como energía eléctrica, agua, telecomunicaciones y el aire acondicionado son evaluados, inspeccionados, probados regularmente para asegurar su buen funcionamiento.

	POLÍTICA	Código:	SGSI-POL-07
		Versión:	1.0
	SEGURIDAD FÍSICA Y DEL AMBIENTE	Aprobado	Oswaldo Veas
		Fecha Aprob.:	20 abril 2020
		Página	6 de 8

- Los equipos de cómputo están protegidos contra fallas por los servicios de apoyo.

4.2.3. Seguridad en el Cableado

- Los cableados de energía eléctrica y telecomunicaciones están protegidos contra la interceptación, interferencia o daños.
- Los cableados de comunicaciones y eléctricos que alimentan a las instalaciones de procesamiento de información, se despliegan a través de canaletas para tal uso.
- Hace inspección física del cableado contra dispositivos no autorizados conectados al cable.

4.2.4. Mantenimiento del Equipamiento

- Realiza un mantenimiento adecuado de todos los equipos informáticos para asegurar su continua disponibilidad e integridad, este debe realizarse de acuerdo a las recomendaciones de intervalos y especificaciones de servicio del proveedor.
- Mantiene registros de los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo.
- Para los equipos que se encuentran en garantía o asegurados se cumple con lo indicado en las pólizas de seguro o certificados de garantía.

4.2.5. Retiro de los Activos

- Todo equipo, información o software no es retirado de las instalaciones de Desysweb S.A.C. sin autorización previa.
- Identifica a todo el personal y usuarios externos que tengan autoridad para permitir el retiro de activos fuera del local de Desysweb S.A.C.

	POLÍTICA	Código:	SGSI-POL-07
		Versión:	1.0
	SEGURIDAD FÍSICA Y DEL AMBIENTE	Aprobado	Oswaldo Veas
		Fecha Aprob.:	20 abril 2020
		Página	7 de 8

- Fija tiempos para los equipos retirados y verificar el cumplimiento de su retorno.
- Se debe registrar la salida y el retorno del equipo.

4.2.6. Seguridad del Equipamiento y de los Activos Fuera de las Instalaciones de la Organización

- Aplica controles de seguridad a todos los equipos que se encuentran fuera de las instalaciones de Desysweb S.A.C., también se aplica a los equipos como computadoras personales, documentos u otros, que se lleven al domicilio o fuera de las instalaciones de Desysweb S.A.C.
- Toma en cuenta las indicaciones del fabricante para la protección de los equipos.
- Aplica controles para los equipos destinados a teletrabajo y sitios temporales.

4.2.7. Seguridad en la Reutilización o Disposición Final de Equipos

- Todo equipo o dispositivo de almacenamiento que contenga información o con derechos de autor es destruido físicamente o elimina o sobre escribirse haciendo uso de técnicas para hacer que la información original sea irrecuperable.
- Los dispositivos de almacenamiento dañados son destruidos físicamente antes de ser desechados.

4.2.8. Equipo Desatendido por el Usuario: Política de Escritorio y Pantalla Limpios

	POLÍTICA	Código:	SGSI-POL-07
		Versión:	1.0
	SEGURIDAD FÍSICA Y DEL AMBIENTE	Aprobado	Oswaldo Veas
		Fecha Aprob.:	20 abril 2020
		Página	8 de 8

- Toda la Información confidencial o crítica del negocio contenida en medios de almacenamiento electrónico o en papel están asegurados bajo llave cuando la oficina este vacía.
- Protege las computadoras o equipos portátiles cuando estén desatendidos ya sea por claves de bloqueo de pantalla, bloqueo de teclado protegidos por contraseña.
- Todo documento que contenga información clasificada como confidencial es retirado inmediatamente de las impresoras, así mismo previene el uso no autorizado de fotocopadoras escáner o cámaras digitales.