DigiPro S.A. de C.V.

Hoja de revisión.

Este documento fue creado conforme a los requerimientos institucionales, revisado por el área de Control y Cumplimiento y aprobado por la Dirección de Tecnologías de Información.

Estamos de acuerdo con su contenido e implementación, en caso de haber cualquier modificación o adición a este documento, es responsabilidad del área emisora indicar la modificación o adición, previa aprobación de las áreas involucradas para evitar errores, incrementar el control interno y/o mejorar la productividad de los departamentos involucrados.

Control de Cambios		
Versión	**Cambios realizados**	**Fecha**
01	Documento de nueva creación	13/01/2025

Contenido

Política de Pantalla y Escritorio Limpio.

Generales

Escritorios Limpios

- Toda vez que un trabajador se ausenta de su lugar de trabajo, junto con bloquear su estación de trabajo, debe guardar en lugar seguro, bajo llave cualquier documento, dispositivo USB o medio óptico removible que contenga información confidencial.
- Las llaves de cajones, gavetas y archiveros no deben estar a la vista.
- Si el trabajador está ubicado cerca de zonas de atención de público, al ausentarse de su lugar de trabajo debe guardar también los documentos y cualquier medio que contengan información de uso interno.
- Al finalizar la jornada de trabajo, el funcionario debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno.
- La información clasificada o confidencial, cuando se imprima, debe ser retirada inmediatamente de las impresoras.
- En centros de operaciones, queda estrictamente prohibido ingresar con celular y/o equipo propio (Laptop, Tablet, IPad, IPod, Consola de Videojuegos, etc.), y cualquier medio de almacenamiento de datos (Discos externos, Memorias externas, etc.) a las áreas donde se encuentre información confidencial o reservada de los clientes.
- En centros de operaciones se realizarán revisiones periódicas aleatorias y diarias de escritorios y pantallas despejados, para garantizar que se practique la protección de los datos internos y confidenciales en cada ubicación de la empresa llenando el reporte "**SGSI-A7-D6AX05 Recorridos de seguridad**"; en caso de localizar una desviación a esta política se procede a levantar un incidente de seguridad.

Pantallas Limpias y Cierre de Sesión por Inactividad

- Las estaciones de trabajo y equipos portátiles deben tener aplicado el estándar relativo a protector de pantalla, de forma que se active el protector definido por DigiPro. El primer periodo de cierre corresponderá a los 5 minutos de inactividad en el PC, tras lo cual se activará el protector de pantalla, con mensajes acordes a las buenas prácticas de seguridad.
- Para desactivar el protector de pantalla y volver al modo normal de funcionamiento de la estación de trabajo, el sistema solicitará nuevamente usuario y contraseña para ingresar al equipo.
- La pantalla de autenticación a la red de la institución debe requerir solamente la identificación de la cuenta y una clave y no entregar otra información.
- El usuario deberá tener el cuidado de no almacenar documentación o información confidencial en el escritorio (pantalla inicial) de la estación de trabajo, se recomienda el uso de carpetas.
- Toda la información contenida en la papelera de reciclaje de Windows debe eliminarse de manera continua, con el fin de evitar que la información sensible pueda ser accedida o robada

- Toda vez que el usuario se ausente de su lugar de trabajo debe bloquear su estación de trabajo de forma de proteger el acceso a las aplicaciones y servicios de la institución. Para ello se recomienda presionar botón Windows + letra L. Al volver el usuario, el sistema solicitará nuevamente usuario y contraseña para ingresar al equipo.
- Después de 20 minutos de inactividad, el equipo deberá entrar en modo hibernación, apagando pantalla y discos duros, en política de ahorro de energía.
- Una vez que el usuario ha terminado su jornada, deberá apagar el equipo.
- En centros de operaciones se realizarán revisiones periódicas, aleatorias y diarias de que las pantallas estén bloqueadas cuando no se encuentre el usuario frente a su estación de trabajo, para garantizar que se practique la protección de los datos internos y confidenciales en cada ubicación de la empresa llenando el reporte "**SGSI-A7-D6AX05 Recorridos de seguridad**"; en caso de localizar una desviación a esta política se procede a levantar un incidente de seguridad.

Protección en Impresoras

- Las impresoras ubicadas en atención o tránsito de público deben estar protegidas de acceso no autorizado.
- Cualquier información que va a ser impresa en cualquier impresora, debe ser retirada de ella en forma inmediata, evitando el acceso a esta información por personas no autorizadas.
- Cuando sea posible y se trate de información confidencial, debe implementarse el control de impresión con el uso de clave por usuario.

Salas y pizarras limpias

- Las salas o áreas de reuniones, salas de conferencias y de capacitación deben quedar limpias de todo el material utilizado.
- Después de las reuniones en que se utilicen pizarras, estas deben quedar limpias de la información que se ha expuesto en ellas.
- En caso de que se utilice una estación de trabajo para presentaciones, si éste fuera de uso común, debe eliminarse la información antes presentada.
- Luego de utilizar salas de reuniones con proyección (PC, data), estos deberán apagarse.
- Mantener en orden su área de trabajo, asegurando que la información reservada o confidencial se encuentre en un lugar seguro cuando se ausente del lugar asignado.
- Recoger de las impresoras los documentos con información reservada o confidencial.
- No dejar expuesta información de uso interno, reservado o confidencial cuando se reciban o encuentre cerca personal externo, sin previa autorización.
- Bloquear el equipo cuando se ausente del lugar asignado.
- Activar el protector de pantalla automático con contraseña a los 5 minutos de inactividad.
- El escritorio o pantalla del equipo no debe tener accesos o archivos con información reservada o confidencial, en la medida de lo posible no debe tener accesos o archivos de uso interno.
- Evitar dejar llaves u otro activo de acceso sobre el escritorio cuando se ausente del lugar asignado.

- Evitar dejar información de uso interno visible o en pizarrones cuando se retire de la oficina o sala de juntas.

Documentos relacionados.

- SGSI-A7-D6AX05 Recorridos de seguridad

Cumplimiento.

- ISO/IEC 27001:2022 / A.7 Controles físicos / A.7.7 Escritorio despejado y pantalla despejada.