1. RESUMEN

Este documento define las políticas y directrices destinadas a asegurar el uso apropiado del puesto de trabajo despejado, así como el bloqueo de pantalla del ordenador o computadora cuando no se encuentre en uso.

2. OBJETIVO

Este documento tiene como objetivo establecer los lineamientos requeridos para fortalecer la protección de la información almacenada tanto en los puestos de trabajo como en los equipos informáticos. Esto se logrará mediante la implementación de mecanismos automáticos de bloqueo en las computadoras cuando no estén siendo utilizadas por los colaboradores de la organización.

3. ALCANCE

Esta política abarca todos los puestos de trabajo y equipos informáticos asignados a los colaboradores de la organización. Cada colaborador es responsable de hacer un uso adecuado de estos recursos, actuando con criterio y en conformidad con las políticas internas de la organización y las normativas locales aplicables.

4. POLÍTICA

La Política de Puesto de Trabajo Desatendido y Bloqueo de Pantalla busca fomentar la concienciación de los colaboradores de la organización sobre la relevancia de la Seguridad de la Información. Para ello, establece directrices orientadas a mantener un entorno laboral organizado, sin documentación, dispositivos de almacenamiento extraíbles u otros elementos vinculados a la información. Además, incluye una normativa de pantalla despejada aplicable a

las estaciones de trabajo y equipos de procesamiento de información asignados a cada empleado.

4.1 NORMAS GENERALES APLICABLES PARA PUESTOS DE TRABAJO DESPEJADO Y BLOQUEO DE PANTALLA

4.1.1 NORMA N°1: PUESTO DE TRABAJO DESATENDIDO Y BLOQUEO DE PANTALLA

Los usuarios deberán observar las siguientes pautas al utilizar computadoras u ordenadores para garantizar la protección adecuada de los equipos cuando estén desatendidos:

- Los dispositivos ubicados en áreas de usuarios, como estaciones de trabajo, o en el Datacenter, como servidores de archivos, deben contar con medidas específicas para prevenir accesos no autorizados en situaciones de desatención.
- Es obligatorio bloquear el equipo de cómputo al abandonar el puesto de trabajo o al finalizar la jornada laboral.
- Cada estación de trabajo, servidor o equipo de Infraestructura de Comunicaciones debe configurarse con un bloqueo automático de sesión tras más de 5 minutos de inactividad.
- Se establecerá un fondo de pantalla uniforme para todos los usuarios.
- Los equipos de cómputo deben apagarse al terminar la jornada laboral, aplicable exclusivamente a estaciones de trabajo o computadoras asignadas a los usuarios finales.

4.1.2 NORMA N°2: PUESTOS DE TRABAJO DESPEJADO

Se deberán considerar las siguientes recomendaciones:

- Mantener el puesto de trabajo organizado y libre de documentos, papeles, revistas u otros elementos que puedan ser vistos por personas no autorizadas.
- Está estrictamente prohibido dejar notas, adhesivos en la pantalla u otros lugares accesibles que contengan información de inicio de sesión o contraseñas, ya que podrían ser observados o manipulados por terceros.
- Garantizar que cualquier documentación que contenga información sensible o confidencial sea resguardada de manera adecuada.
- justifiquen nuevos accesos y sean aprobados por el Jefe inmediato y el Comité de Gestión de Seguridad de la Información (CGSI).

5. CUMPLIMIENTO DE POLÍTICA

5.1 MEDICIÓN DEL CUMPLIMIENTO

La organización realizará un seguimiento y verificación del cumplimiento de esta política mediante una variedad de métodos, incluyendo:

- Visitas periódicas
- Monitoreo de video
- Informes generados por herramientas comerciales
- Auditorías internas y externas
- Inspecciones

Los resultados de estas actividades serán comunicados al propietario de la política y al gerente de la unidad de negocio correspondiente, con el fin de garantizar el cumplimiento y la mejora continua de la política.

5.2 EXCEPCIONES

Cualquier excepción a esta política deberá ser sometida a aprobación previa por parte del Gerente de área correspondiente y el Grupo Interdisciplinario de Seguridad de la

Información (GISI), quienes evaluarán y autorizarán las excepciones de acuerdo con las necesidades y riesgos de la organización.

5.3 INCUMPLIMIENTO

Cualquier empleado que incumpla o viole esta política estará sujeto a medidas disciplinarias, que pueden incluir desde advertencias hasta el despido, dependiendo de la gravedad de la infracción y la discreción de la organización.

6. APROBACIÓN

Elaborado por	Verificado por	Aprobado por
Nombre **Oficial de Seguridad de la Información** Fecha:	Nombre **Gerente Administrativo** Fecha:	Nombre **Gerente General** Fecha: