1. RESUMEN

El acceso remoto a la organización resulta fundamental para garantizar la productividad de los recursos internos. Por ello, considerando que en numerosos casos dicho acceso se realiza desde redes potencialmente comprometidas o con un nivel de seguridad inferior al de la red interna de la organización, es imprescindible observar la presente Política de Seguridad de Teletrabajo, diseñada para mitigar de manera efectiva los riesgos externos asociados.

2. OBJETIVO

El objetivo de esta política es establecer directrices y condiciones para acceder a la red de la organización desde redes externas. Estas pautas están orientadas a minimizar los riesgos potenciales asociados al uso no autorizado de los recursos organizacionales. Entre los posibles perjuicios se encuentran la pérdida de información confidencial o sensible, afectación de la propiedad intelectual, daños a la reputación, compromisos en sistemas críticos y sanciones financieras u otras responsabilidades derivadas de dichas pérdidas.

3. ALCANCE

Esta política abarca a todos los empleados que utilicen una computadora o estación de trabajo propiedad de la organización para acceder a los recursos locales. Quedan excluidos de las conexiones remotas cualquier dispositivo que no sea una computadora o estación de trabajo previamente registrada en los accesos autorizados. Además, esta política se aplica a las conexiones remotas utilizadas para actividades laborales, como la lectura, escritura o envío de correos electrónicos, así como la consulta de recursos internos. Se incluye dentro de su alcance todas las implementaciones técnicas de acceso remoto utilizadas para conectarse a la organización.

4. POLÍTICA

Los empleados de la organización que cuenten con privilegios de acceso remoto a la red corporativa deben asegurarse de que su conexión remota sea tratada con el mismo nivel de seguridad que la conexión en el sitio del usuario dentro de la organización.

Las normas relacionadas son las siguientes:

4.1 NORMAS GENERALES APLICABLES PARA EL TELETRABAJO

4.1.1 NORMA N°1

El acceso remoto seguro debe ser rigurosamente controlado mediante configuraciones con algoritmos de cifrado, como las redes privadas virtuales (VPN), y autenticación robusta. Para esto, se ha establecido un procedimiento de configuración en Fase 1 y Fase 2 para la conexión del cliente VPN, el cual debe instalarse en las computadoras o estaciones de trabajo. Si es necesario, los detalles de esta configuración pueden ser consultados con el personal del área de Soporte Técnico de la organización.

4.1.2 NORMA N°2

El uso de acceso remoto para la utilización de recursos externos debe ser aprobado previamente por el Gerente del área correspondiente, después de ser revisado por el Grupo Interdisciplinario de Seguridad de la Información (GISI).

4.1.3 NORMA N°3

El acceso a las computadoras o estaciones de trabajo se realizará únicamente mediante la inclusión y autorización de la Mac-Address del dispositivo. La lista completa de estos dispositivos autorizados será añadida a la regla de Firewall, permitiendo el acceso a los recursos internos según las áreas de acceso previamente autorizadas.

4.1.4 NORMA N°4

Cuando un usuario autorizado utilice un equipo de la organización para conectarse remotamente a la red corporativa, deberá asegurarse de que el host remoto no esté conectado a ninguna otra red simultáneamente, salvo a redes personales completamente bajo su control o el control total del usuario.

4.1.5 NORMA N°5

Todos los dispositivos conectados a las redes internas de la organización mediante acceso remoto deben contar con el software antivirus más actualizado implementado por la organización.

4.1.6 NORMA N°6

Al conectarse y consumir recursos internos de la organización, el usuario se compromete a navegar exclusivamente a través de redes seguras de acceso externo, como Internet. Al acceder mediante cliente VPN, las políticas de navegación serán las mismas que si estuviera dentro de la organización. Además, el registro de navegación será enviado a una consola de logs, que podrá ser revisado posteriormente para generar el historial de navegación del usuario, si es necesario.

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: