LYNX TEC

Política de Seguridad de la Información

GENERALIDADES

LYNX TECNOLOGIA SAS cuenta con computadores provistos de licencia de Antivirus debidamente licenciados.

El acceso a los servidores de los clientes para el soporte remoto se realiza mediante dos opciones:

- Contamos con un computador dedicado, el cual no cuenta con programas de ofimática, solo con el programa **Anydesk** para acceder a los computadores de los clientes que no cuentan con accesos VPN (conexión segura y cifrada).
- El ingreso a esos servidores solo lo hace el personal autorizado por LYNX TECNOLOGIA SAS, en este caso es el coordinador de soporte, y se hace de forma asistida por el cliente.
- Dos computadores para los Clientes que cuentan con una conexión segura y cifrada **VPN**, y un usuario y clave con perfiles de acceso acorde a sus requerimientos de seguridad. Este VPN es instalado por el mismo cliente en nuestros computadores donde inscriben la MAC de nuestro equipo para garantizar que el acceso sea realizado desde un computador único.

GARANTÍA DE SEGURIDAD

El acceso a través de Anydesk solo lo realiza el coordinador de soporte, quien lo hace de forma asistida por el cliente. Adicionalmente, contamos con:

1. Software licenciado de antivirus en todos nuestros computadores.
2. Computadores dedicados para ingreso a sistemas remotamente.
3. Software licenciado de Anydesk.
4. Entrenamos a nuestros funcionarios en el correcto manejo de los datos con seguridad y manejo de la información, de nuestro cliente en procedimientos de mantenimiento y soporte al sistema.
5. Para acezar a la información, se realiza a través de la aplicación instalada por el cliente autenticando previamente el usuario y una clave.

CONTROLES TÉCNICOS Y ADMINISTRATIVOS

La integridad de la base de datos se garantiza mediante controles de acceso con privilegios mínimos, autenticación fuerte, autorización granular, uso estricto de sentencias parametrizadas, registro y auditoría de cambios. Adicionalmente, se mantiene integridad transaccional ACID manipulación.

MANEJO DE BRECHAS

Ante la detección de una amenaza se realiza el siguiente protocolo:

1. Se informa de los hechos al Ingeniero de Seguridad.
2. Se procede a aislar el equipo comprometido.
3. El Ingeniero de Seguridad realiza una revisión previa del evento e informa al profesional especializado según el caso.
4. El profesional especializado realiza un análisis detallado del evento,
5. Si se detecta una amenaza positiva, se informa al cliente y/o a las autoridades correspondientes.
6. Se cancela el correo y/o se remplaza el equipo según sea el tipo de afectación.

HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	Abril 2025	Creación de Formato