La presente Política de Seguridad de los Accesos establece las directrices para la gestión, control y uso adecuado de los accesos a los sistemas de información, aplicaciones, redes y activos tecnológicos de BUSINESS SOLUTION CONSULTORES S.A.C., con el fin de prevenir accesos no autorizados y proteger la información.

1. Gestión de cuentas y privilegios de acceso

- La creación, modificación o eliminación de cuentas de usuario y privilegios de acceso deberá ser autorizada por el jefe de área correspondiente y validada por la Gerencia o el área responsable.
- Las solicitudes de correos electrónicos, accesos remotos, sistemas de tickets, servidores u otros recursos tecnológicos deberán ser gestionadas a través de los canales definidos y contar con la autorización correspondiente.
- Al recibir una cuenta de usuario, el personal declara conocer y aceptar las políticas y procedimientos de seguridad de la información, así como las responsabilidades asociadas al uso de dicha cuenta.
- No se concederán cuentas de usuario a personas ajenas a la organización. En caso excepcional, se podrán otorgar cuentas temporales a terceros (proveedores, consultores u otros), previa autorización del jefe de área y Gerencia correspondiente.
- Los jefes de área deberán definir y comunicar al área de TI los privilegios de acceso requeridos por cada usuario, de acuerdo con el principio de mínimo privilegio.
- Las cuentas temporales otorgadas a terceros deberán ser revocadas o eliminadas una vez finalizado el servicio contratado.

2. Control de accesos externos y de invitados

- A clientes, proveedores o visitantes que requieran acceso a Internet se les proporcionará acceso restringido mediante red de invitados, sin acceso a la red interna de la empresa.
- El acceso de dispositivos externos a la red interna estará prohibido, salvo autorización expresa del jefe de área y del área de TI, y bajo los controles de seguridad definidos.
- El área de TI podrá verificar que los equipos de terceros cuenten con medidas básicas de seguridad, tales como antivirus activo y actualizado.

3. Gestión de contraseñas

- La contraseña es de uso personal e intransferible, y el usuario es responsable de su confidencialidad y custodia.
- Las contraseñas iniciales asignadas deberán ser cambiadas obligatoriamente en el primer inicio de sesión.

- Las contraseñas no deberán ser almacenadas en forma legible ni compartidas con otros usuarios.
- En caso de sospecha de compromiso de la contraseña, el usuario deberá comunicarlo inmediatamente al área de TI para su restablecimiento.
- Las contraseñas deberán cumplir con los requisitos mínimos de seguridad definidos por el área de TI, tales como:
- Longitud mínima de 8 caracteres.
- Combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
- No se deberán reutilizar contraseñas previamente empleadas.

4. Bloqueo de sesiones y revocación de accesos

- Las sesiones de usuario deberán bloquearse automáticamente tras un período de inactividad.
- El área de TI deberá revocar de manera oportuna los accesos y privilegios cuando el usuario cambie de funciones, cese su relación laboral o por instrucción de la Gerencia o Recursos Humanos.
- En casos de desvinculación, los accesos deberán ser deshabilitados de acuerdo con el procedimiento establecido.

El área de TI realizará revisiones periódicas de los accesos a sistemas, correos, servidores y otros activos tecnológicos, con el fin de verificar su vigencia y adecuación a las funciones del usuario.

Gerente General