POLÍTICA DE CONTROL DE ACCESO

DESYSWEB

Lima - Perú

CONTENIDO

1. OBJETIVO

Controlar el acceso a la información y a las instalaciones de procesamiento de información de Desysweb S.A.C.

2. ALCANCE

Aplica a todo el personal que labora en Desysweb S.A.C.

3. DEFINICIONES

Están detalladas en la Norma Internacional ISO/IEC 27000:2016 "Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Información general y vocabulario".

4. POLÍTICA

4.1. Requisitos de Negocio del Control de Acceso

4.1.1. Política de Control de Acceso

- Establece controles de acceso, según los requisitos de Desysweb S.A.C. para la seguridad de la información.
- Los propietarios de los activos de información definen las reglas de control de acceso, derechos y restricciones para el personal y proveedores de Desysweb S.A.C. a sus activos, considerando los riesgos asociados de seguridad de la información.
- Los controles de acceso son tanto para accesos lógicos como físicos y deben basarse en los roles del personal.

4.1.2. Acceso a las Redes y a los Servicios de Red

- El personal solo tiene acceso a redes y servicios de red a los que fueron específicamente autorizados a utilizar.

- Todo el personal o proveedor que requiere acceder a la red y servicios de red debe contar con las autorizaciones respectivas de los propietarios de los activos.

4.2. Gestión de Acceso del Usuario

4.2.1. Registro y Baja de Usuarios

- Implementa un proceso formal para el registro y baja de usuarios para permitir la asignación y eliminación de accesos.
- Asigna una identificación IDs única para cada usuario que permita vincularlo con sus accesiones y sean responsables de ellas.
- Elimina o desactiva inmediatamente los IDs de los usuarios cesados o que se desvinculen de Desysweb S.A.C.
- Los IDs redundantes deben ser desactivados, eliminados y asegurarse de que no vuelvan a otorgarse a otros usuarios.

4.2.2. Gestión de Acceso a los Usuarios

- Los Gerentes y/o Jefes son los encargados de autorizar y solicitar el acceso del personal a los recursos de tecnología de información. Asimismo, informan y solicitan al área de TI la cancelación de accesos en caso que un trabajador deje de pertenecer a Desysweb S.A.C. o cuando sus funciones ya no lo requieran.
- El área de TI asigna un identificador (cuenta) único y exclusivo a toda persona que haga uso de los activos de información ya sea de forma temporal o permanente y que le permita contar con el mínimo acceso autorizado para el normal desarrollo de sus actividades.
- Controla que no se compartan identificadores entre diferentes usuarios, para ello deben definirse políticas de control a nivel

sistema operativo y/o de red, de manera que se pueda detectar duplicidad de sesiones de usuarios.

4.2.3. Gestión de Derechos de Acceso Privilegiados

- Está restringido y controlado la asignación y uso de los derechos de acceso privilegiados.
- Está identificado los derechos de acceso privilegiado asociados a cada sistema o proceso, así como los usuarios a los que se les está otorgando los privilegios.
- Está definido los requisitos para la expiración de los derechos de acceso privilegiados.
- Se revisa constantemente las cuentas de los usuarios con los accesos privilegiados y si están alineados a sus funciones.

4.2.4. Gestión de la Información de Autenticación Secreta de los Usuarios

- Está controlada toda asignación de autenticación secreta con un proceso formal.
- Se verifica la identidad del usuario antes de proporcionarle la información de autenticación secreta nueva, sustitutiva o temporal.
- La entrega de la autenticación temporal es en forma segura y única para cada individuo.

4.2.5. Revisión de los Derechos de Acceso de Usuario

- Los derechos de acceso de los usuarios son revisados a intervalos regulares y/o luego de cualquier cambio.

4.2.6. Eliminación o Ajuste de los Derechos de Acceso

- Los derechos de acceso de todo el personal o usuarios de proveedores a información e instalaciones de procesamiento de

información son eliminados como consecuencia de la desvinculación de su empleo, contrato o acuerdo o ser ajustado ante cambios.

- Se reducen o eliminan todos los derechos de acceso a la información y los activos asociados a las instalaciones de procesamiento de información antes de la finalización del empleo o cambio.

4.3. Responsabilidades del Usuario

4.3.1. Uso de la Información de Autenticación Secreta

- Se da a conocer a todos los usuarios sobre las prácticas de Desysweb S.A.C. respecto al uso de la información de autenticación secreta.
- Todo usuario mantiene en secreto la información de autenticación confidencial, asegurando que no se divulgue a otras partes, incluyendo personal de autoridad.
- Toda información de autenticación secreta es segura, evitando el uso de papel u otros registros que sea fácil de obtener.
- Los usuarios cambian la información de autenticación secreta cuando exista indicios de su posible compromiso.
- Las contraseñas tienen un suficiente largo mínimo, que no es fácil de adivinar, que no son palabras que se encuentran en el diccionario, combina letras mayúsculas, minúsculas, números y otros caracteres que se encuentran en el teclado incluyendo los espacios.
- Los usuarios no deben compartir contraseñas, no usar la misma información de autenticación para propósitos comerciales y no comerciales.

4.4. Control de Acceso al Sistema y a las Aplicaciones

4.4.1. Restricción de Acceso a la Información

- Todo acceso a la información y a las funciones del sistema de aplicaciones es restringido.
- Todos los derechos de acceso ya sea de lectura, escritura, borrar y ejecutar son controlados, así como los datos y aplicaciones que son accedidos por el usuario.
- Los accesos lógicos y físicos son controlados para aislar datos de aplicaciones o sistemas, aplicaciones sensibles de Desysweb S.A.C.

4.4.2. Procedimientos Seguros de Inicio de Sesión

- El inicio de sesión es controlado por un procedimiento seguro de (log-on).
- No muestra identificación de aplicación alguna o mensajes de ayuda antes de finalizar el proceso de inicio de sesión.
- Cancela sesiones inactivas luego de un periodo determinado en las aplicaciones críticas y sistemas operativos.
- Todo intento fallido y exitoso de inicio de sesión queda registrado.
- En caso de alguna posible intrusión fallida o exitosa de los controles de inicio de sesión genera un evento de seguridad.

4.4.3. Sistema de Gestión de Contraseñas

- El sistema de gestión de contraseñas es interactivo.
- Todas las contraseñas e identificaciones (IDs) son individuales, permitiendo a los usuarios seleccionar y cambiar sus contraseñas, incluyendo confirmación.

- El personal usa contraseñas de calidad, cambia de contraseñas periódicamente, evita la reutilización de contraseñas, para esto se mantiene un registro de las contraseñas usadas anteriormente.
- Se almacena y transmite las contraseñas en forma protegida.

4.4.4. Uso de Programas Utilitarios Privilegiados

- El uso de programas utilitarios es restringido y es limitado el uso solo para usuarios autorizados y asimismo son también controlados.
- Todo programa utilitario pasa por un proceso de identificación, autenticación y autorización de uso, así como su registro, definición y documentación.
- Todo programa innecesario es desactivado, eliminado.