POLÍTICA DE GESTIÓN DE DISPOSITIVOS MÓVILES Y REMOVIBLES

DESYSWEB

Lima - Perú

CONTENIDO

1. OBJETIVO

Definir las políticas para el uso de dispositivos móviles o removibles por parte de los colaboradores de la Compañía.

2. ALCANCE

Esta política aplica para cualquier colaborador, tercero o proveedor de Desysweb S.A.C. que requiera hacer uso de una estación de trabajo, dispositivo móvil o dispositivo removible

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".

- Antivirus: Software de detección y eliminación de virus informáticos conocidos como "malware".
- DISCOS DUROS EXTERNOS: Unidad removible con mayor capacidad de almacenamiento de datos lógico, en comparación con las memorias USB.
- MDM: Software de gestión de dispositivos móviles, permite a la Compañía habilitar de forma segura el uso de dispositivos y aplicaciones móviles por parte de los colaboradores.
- Software de Gestión de Activos: Software denominado Desktop Central, usado para el registro de todos los activos fijos (incluyendo dispositivos móviles) gestionados por el Área de TI.
- USB: Memoria flash externa de almacenamiento de datos lógicos

4. POLÍTICA

4.1. Tipos de Dispositivos Móviles

4.1.1. Dispositivos Móviles

Dentro de los dispositivos móviles que suministra el Área de TI al personal de la organización, se encuentran: Celulares o Móviles y Laptops.

4.1.2. Dispositivos Removibles

Dentro de los dispositivos móviles que suministra el Área de TI al personal de la organización, se encuentran: Discos Duros Externos.

4.2. Dispositivos Móviles

4.2.1. Controles de seguridad

Los dispositivos móviles deberán contar con un software de gestión de configuración (MDM) el cual es administrado por el Área de TI. Este software controla los parámetros técnicos de seguridad a nivel del sistema operativo Android y iOS, así como la gestión de los datos almacenados para evitar manipulación por atacantes o terceros.

Las configuraciones realizadas a través del MDM deberán encontrarse alineadas con las buenas prácticas definidas por la organización para la mitigación de riesgos de seguridad de información. Cualquier desviación a las configuraciones recomendadas por el Área de TI, deberá ser documentada y autorizada por el Gerente de TI y Proyectos.

4.2.2. Configuración de MDM

Las configuraciones del software MDM son responsabilidad del Área de TI y serán revisadas de manera recurrente confirmando que todos los activos registrados en el software de Gestión de Activos se encuentren debidamente controlados a través del MDM.

4.2.3. Uso de dispositivos móviles personales

No se encuentra autorizado el uso de dispositivos móviles personales para el almacenamiento de información o conexión a la red de Desysweb S.A.C. Las excepciones que puedan existir deberán ser autorizadas por el Gerente de TI y Proyectos y los dispositivos móviles personales estarán obligatoriamente sujetos a las configuraciones mencionadas en el punto 4.1.3.

4.2.4. Incumplimientos ante alteración de MDM

En caso de que el usuario del dispositivo móvil realice una alteración del software MDM instalado, deberá encontrarse sujeto a las penalidades o amonestaciones

definidas por el Área de TI en conjunto con el área de Recursos Humanos. Para más información, ver la *SGSI-POL-15 Política uso Aceptable de Activos de Informática.*

4.2.5. Reporte ante robo o perdida

En caso de que el usuario del dispositivo móvil haya sufrido la pérdida o hurto del dispositivo, el usuario deberá reportar inmediatamente al Área de de TI indicando la criticidad de la información contenida en el dispositivo. Para más información sobre la clasificación de la información, ver *SGSI-POL-01 Política de Seguridad de la Información.*

4.3. Dispositivos Removibles

4.3.1. Solicitudes de habilitación de puertos USB

Para hacer uso de dispositivos removibles, el usuario deberá contar con la autorización de la Jefatura Inmediata y explicar el sustento de la solicitud. Esta solicitud deberá ser aprobada por el Gerente de IT y Proyectos. Cabe resaltar, que las solicitudes de habilitación de puertos USB son excepcionales dado que las configuraciones básicas de las laptops o estaciones de trabajo de todo colaborador cuentan con el bloqueo automático de puertos USB.

4.3.2. Controles de seguridad

Las estaciones de trabajo o laptops que sí se encuentren autorizados para la conexión de dispositivos removibles, de acuerdo con lo estipulado en el punto 4.3.1, deberá contar obligatoriamente con la instalación del software de protección de datos Sophos y BitLocker, el cual encriptará los archivos copiados en los dispositivos removibles. En caso existan excepciones, estas deberán ser documentadas y aprobadas por el Gerente de TI y Proyectos.

4.3.3. Reporte ante robo o pérdida

En caso de que el usuario del dispositivo removible haya sufrido la pérdida o hurto de este, deberá reportar inmediatamente al Área de TI indicando la criticidad de la información contenida en el dispositivo. Para más información

sobre la clasificación de la información, ver *SGSI-POL-01 Política de Seguridad de la Información*.

4.4. Otros medios de almacenamiento

4.4.1. Controles de seguridad en laptops

Dado que las laptops son dispositivos móviles asignados a colaboradores que transitan o movilizan el equipo por razones laborales, estas se encuentran expuestas a riesgo de pérdida o hurto. Los discos duros de estos dispositivos se encuentran encriptados por la solución BitLocker, lo cual reducirá el riesgo de extracción de información contenida en el dispositivo.

4.4.2. Reporte ente robo o pérdida

En caso de que el colaborador al que se le asignó una laptop haya sufrido la pérdida o hurto de esta, deberá reportar inmediatamente al Área de TI indicando la criticidad de la información contenida en el dispositivo. Para más información sobre la clasificación de la información, ver *SGSI-POL-01 Política de Seguridad de la Información*.

4.5. Protección de dispositivos

4.5.1. Ejecución de antivirus

Previo al uso de dispositivos removibles, el usuario deberá ejecutar un análisis de antivirus Sophos para confirmar que el dispositivo no cuente con malware o algún virus informático que pueda poner en riesgo la integridad de la información contenida en la estación de trabajo o laptop.

4.5.2. Alteración de la configuración de antivirus

No se encuentra permitido la deshabilitación o alteración de la configuración del software de antivirus Sophos instalado en la estación de trabajo o laptop del colaborador.

En caso el Área de TI evidencie la alteración de alguna configuración crítica, el colaborador deberá encontrarse sujeto a las penalidades o amonestaciones definidas por el Área de TI en conjunto con el área de Recursos Humanos. Para

más información, ver la *SGSI-POL-15 Política uso Aceptable de Activos de Informática.*

4.5.3. Verificación de estado de antivirus

Para minimizar los riesgos de seguridad de información relacionados a la infección por malware, el Área de TI realiza una revisión bimestral sobre el estado de configuraciones de antivirus en todas las estaciones de trabajo y laptops conectadas a la red de la compañía confirmando su adecuada disponibilidad.