maximobility.

ESTÁNDARES CORPORATIVOS DE SEGURIDAD DE DATOS

INTRODUCCIÓN

Este documento describe la política de seguridad de Maxi Mobility, tanto a niveles de hardware, como de software. El tener una política unificada de seguridad persigue varios objetivos:

- Asegurar que los datos que manejamos, tanto privados de la empresa (financieros, fiscales, propietarios, de ventas), como los datos privados de nuestros clientes y de nuestros empleados están seguros ante posibles intentos de robo, copia o utilización inapropiada.
- Garantizar a nuestros clientes, inversores y partners que el uso de datos dentro de nuestra compañía cumple o excede los estándares de seguridad de una empresa moderna.
- Ofrecer a todos los trabajadores de Maxi Mobility las herramientas necesarias para que puedan realizar su trabajo con con confianza de que lo están realizando en un entorno seguro
- Unificar todos los procedimientos de seguridad bajo un mismo techo, simplificando su cumplimiento a la vez que se refuerzan los pilares en los que basamos la seguridad de los datos.

RESUMEN

La política standard de seguridad está dividida en varias áreas:

- Medidas básicas de ciberseguridad
- Estándares de sistemas corporativos
- Medidas de seguridad básicas dentro del equipo de desarrollo
- Cumplimiento de DGPR y Prevención DLP
- Comité de seguridad digital corporativa

Estas medidas de seguridad son fundamentales para que una compañía como la nuestra pueda garantizar la integridad y privacidad de los datos, pero la parte más importante una política de seguridad es que la

maximobility.

cumplamos. La primera y más importante línea de defensa que tiene Maxi Mobility contra posibles intrusiones o intentos de robo de datos es nuestros trabajadores. Os pedimos por favor que leáis con detenimiento este documento y seáis consistentes en la aplicación del mismo.

MEDIDAS BÁSICAS DE CIBERSEGURIDAD

En esta sección podéis encontrar las medidas más básicas de seguridad que son comunes a todos los usuarios de Maxi Mobility. Estas medidas, aunque en muchos casos simples y evidentes, son el arma más importante que tenemos para evitar fugas de datos o intrusiones en nuestros sistemas.

1. Tus claves de TODOS los sistemas son personales e intransferibles, no las compartas con nadie, ni siquiera IT o tu jefe/supervisor. IT nunca te pedirá tu contraseña.

2. JumpCloud es nuestro sistema de SSO (Single Sign On). En este momento JumpCloud controla la contraseña de Google, Dropbox, VPN y en algunos casos Tableau. En el futuro la mayoría de las aplicaciones se gestionarán desde aquí. Tu contraseña caducará cada 90 días y tiene que tener una complejidad de 8 caracteres, una mayúscula, una minúscula y un número. El despliegue de JumpCloud se está realizando por países, si crees que en tu localidad ya se ha desplegado y no tienes todavía Jumpcloud habilitado, puedes escribir en el canal de Slack #it_security para que te lo habilitemos.

3. Asegúrate de que tienes la "identificación de dos pasos" habilitada en Google (Si intentas acceder desde un dispositivo nuevo, tu teléfono te pedirá permiso). Si no la tienes habilitada, contacta con IT en el canal #it_security. A partir de Q2 2019 no podrás acceder a Gsuite sin 2FA habilitado

4. Bloquea tu equipo cuando te levantes, Si no lo haces, una vez habilitado en tu dispositivo, JumpCloud lo hará por ti.

maximobility.

5. Si tienes correo en el teléfono, es **OBLIGATORIO** PIN o patrón/huella. Si tu terminal es de empresa, tendrás el MDM de google instalado. Si lo pierdes o te lo roban, repórtalo a IT inmediatamente. Para el que quiera tener el MDM habilitado en sus teléfonos personales (medida extra de seguridad contra robos, a nivel profesional y personal), se puede habilitar también pidiéndolo a través del canal #it_security.

6. Eres responsable de lo que ocurra con la información que compartas digitalmente, a efectos laborales y legales. Esto significa que si compartes información con personas no autorizadas, las consecuencias de su uso son responsabilidad tuya.

7. Mucho cuidado con el Phising… Si no conoces al remitente de un correo electrónico, o no esperas el correo, NUNCA abras links o adjuntos. Cualquier link que pida datos financieros, fiscales o de identidad debe ser tratado como “sospechoso”. En caso de encontrar un correo de este tipo, es importante reportarlo a global.it@cabify.com o en el canal de slack #it_security

8. Tened mucho cuidado con quién y a qué nivel de permisos compartes documentos. La herramienta standard para compartir ficheros con externos es Dropbox Enterprise. Compartir ficheros a través de drive se irá deshabilitando progresivamente durante 2019.

9. No compartas información de nombres de servidores, contraseñas o código en general en ningún foro público o privado en Internet... NUNCA.

10. No instales ninguna aplicación por API contra google sin consultar primero (Esto significa que si te pide tu cuenta de cabify para darte acceso, usa API). Se harán barridos periódicos de las aplicaciones conectadas por API, y cortaremos lo que no conocemos... por lo que las aplicaciones no permitidas dejarán de funcionar.

maximobility.

ESTÁNDARES DE SISTEMAS CORPORATIVOS

La homogeneidad de hardware y Software es un importante en un entramado de seguridad, cuanto más homogéneos son los sistemas que tengamos, menos posibles agujeros de seguridad tendremos. Con esto en mente, hemos diseñado estos estándares de sistemas, que deben ser seguidos salvo autorización expresa por parte de IT Global:

1. Los equipos informáticos con los que trabajamos no deben estar anticuados, por lo que la vida útil límite de estos equipos no debe ser sobrepasada (en años):
    a. Laptops: 3 recomendado, 5 máximo
    b. Switches: 4 recomendado, 6 máximo
    c. Firewalls: 4 recomendado, 6 máximo
    d. Tablets: 2 recomendado, 4 máximo
    e. Servidores: 3 Recomendado y máximo, deben transicionar a la nube en vez de reemplazarse
2. Los sistemas operativos de los Laptops aceptados son:
    a. Windows: Windows 10 Build 1709 o más moderno
    b. Apple: MacOS 10.12 Sierra o mas moderno
    c. Linux: Ubuntu 16.04 o más moderno
    d. Chrome OS: No version needed
3. Todos los sistemas Apple, Windows y Linux deberán tener habilitadas las actualizaciones automáticas, siendo su la instalación automática obligatoria por lo menos una vez por semana.
4. Todos los sistemas Apple y windows deben tener el Antivirus/anti-spyware corporativo instalado, en estos momentos el standard es Palo Alto Traps. Si tu dispositivo no lo tiene, comunicarlo en el canal #it_security.
5. Todos los sistemas que trabajan en remoto deben tener disponible la VPN Globalprotect Cloud service desplegada en sus equipos y activada cuando estén fuera de la oficina
6. En Q4 2019 se lanzará en remoto la encriptación de los discos duros de todos los dispositivos, ya sean Windows o Mac… la clave desencriptado se guardará en un repositorio propiedad de la empresa.

maximobility.

7. Trato del hardware de la empresa:
    a. Los usuarios son responsables del trato que den a los dispositivos de la empresa. Se aceptará el desgaste lógico por uso de los dispositivos así como posibles accidentes (ejemplo, se le ha caído un vaso de agua). La reparación por accidente será a cargo de la empresa
    b. No se aceptará el trato negligente de los equipos o accidentes que se pudieran ser prevenidos (Ejemplo, se ha caído a la piscina). LA reparación en caso de negligencia será a cargo del usuario.
    c. El equipo deberá ser devuelto a IT en condiciones similares a las que se recibió, esto significa que si se han puesto pegatinas o accesorios, es responsabilidad del usuario quitarlas antes de devolver el equipo.
    d. En caso de robo, es necesario presentar una denuncia de forma inmediata ante la policía, y presentar esta denuncia lo antes posible ante IT. Es fundamental informar en cuanto se conozca el robo a IT para bloqueo de cuentas. El remplazo de un equipo robado corre a cuenta de la empresa, pero un segundo equipo robado en un periodo menos de 2 años correrá a cargo del usuario, ya que constituye poco respeto por parte del trabajador del material de la empresa.
8. El uso de memorias externas USB ha de ser limitado a memorias que se encuentran encriptadas. Toda transferencia de datos a externos deberá ser realizada a través de los métodos aprobados (Dropbox) y nunca a través de memorias externas. Estas deben limitarse a transferencias de datos entre dispositivos internos de la compañía.
9. Los laptops aceptados en la compañía son los siguientes:
    a. Standard (Equipo base): HP Probook 440: i5, 8gb ram, 128gb SSD, FullHD, Windows 10 Pro (o similar si no es económicamente viable).
    b. Performance (Usuarios que necesitan potencia): HP Elitebook 840, i7, 16gb Ram, 256 SSD, Wind10 pro (o similar si no es económicamente viable).
    c. Executive (Heads, GMs, C-Level) : HP X360 1030: i5 8gb RAM, 256 SSD, Win10 Pro (o similar si no es económicamente viable).

maximobility.

   d. KAM (Team Members con función ventas a clientes clave): Microsoft Surface Pro: i5, 8gb Ram, 128 SSD, Win10 Pro
   e. Development (or approved by Global Head/GM): Apple Macbook pro 13, i7, 16gb RAM, 256 SSD

10. Ningún software, salvo el aprobado por el departamento de IT Global, puede ser instalado en los equipos de la empresa. Las únicas excepciones a esta regla serán los software utilizados por el equipo de desarrollo, cuya instalación y responsabilidad recae sobre el equipo de producto.
11. Las copias locales de datos deben ser la excepción, no la norma. La forma adecuada de trabajar en Maximobility es en la nube, específicamente en Google Drive.

MEDIDAS DE SEGURIDAD AÑADIDAS PARA EL EQUIPO DE DESARROLLO

1. Todos los equipos del equipo de producto deben estar encriptados con sistemas de como mínimo 256 bits.
2. Todos los sistemas internos con conexión a internet deben estar protegidos a través de un proxy con autenticación Oauth2.
3. En caso de pérdida o robo de cualquier equipamiento que sea parte de nuestro equipo de producto, es imperativo reportarlo de forma inmediata al correo panic@cabify.com
4. En caso de pérdida, robo o sospecha de problema de credienciales es imperativo reportarlo de forma inmediata al correo panic@cabify.com
5. Todo comunicado al correo de pánico resultará en el bloqueo por defecto de la cuenta reportada e inicio de investigación de seguridad, por lo que hay que estar relativamente seguro/a de que se ha producido un incidente.
6. Todas las contraseñas deben estar generadas por el gestor de contraseñas seguras automático que tenemos estandarizado dentro del equipo de producto.

maximobility.

CUMPLIMIENTO DE GPDR Y PREVENCIÓN DE DLP

La normativa de protección de datos Europea que entró en vigor en 2018, conocida por GDPR, es una normativa de obligado cumplimiento por parte de las empresas y de sus empleados. Es muy importante que sigamos unas normas básicas para cumplir con ella.
La idea principal de la GDPR es que los datos personales de las personas no deben ser compartidos, almacenados o tratados sin el consentimiento expreso de la persona dueña de estos datos, y que las empresas y/o empleados seguirán unas normas básicas con el tratamiento de estos datos que garantizan que estos datos no se pierdan, sean accedidos por personas no autorizadas o almacenados sin razón.

1. Las medidas de protección de datos personales se deben tratar con el mismo cuidado para información tanto de clientes como de empleados
2. Los empleados han de manejar la información privada con cuidado, no guardando nunca información personal (salud, financiera, contacto…) donde pueda ser accesible para personas no autorizadas
3. La cantidad de información personal utilizada y almacenada ha de ser la menor posible para el cumplimiento de la tarea a realizar
4. La información personal no debe ser compartida con nadie, ya sea persona física o jurídica, fuera de la organización Maxi Mobility sin que antes haya firmado un documento donde certifique que se adhiere a la normativa vigente
5. Nuestros sistemas, sean internos o contratados, han de tener la capacidad para borrar o anonimizar la información personal que sea requerida en un plazo máximo de 14 días para información no financiera.
6. Los empleados deben abstenerse de enviar datos de carácter personal por correo electrónico salvo con consentimiento expreso de la persona cuyos datos están siendo compartidos.
7. Todos los datos en las carpetas compartidas de la empresa son auditados de forma automática, y datos personales (De salud, financieros, fiscales o de contacto) compartidos fuera de la organización o abiertos a todos los usuarios de Maxi Mobility S.L.U. serán borrados automáticamente sin previo aviso.

maximobility.

8. Cualquier persona con conocimientos de una fuga de datos, ya sean de carácter personal tanto de clientes como de empleados, como propietarios y confidenciales de la empresa, ha de reportar esta fuga inmediatamente al correo electrónico dpo@cabify.com

COMITÉ DE SEGURIDAD DIGITAL CORPORATIVA

En Maxi Mobility nos tomamos muy en serio la seguridad de datos tanto de nuestros clientes como nuestros empleados, por lo que se ha creado un comité de seguridad digital corporativa que se reúne como mínimo una vez al trimestre, y que tendrá un reporte del estado de la seguridad mensual distribuido.

1. El comité de seguridad estará coordinado por el departamento de IT y el de producto, con el responsable de seguridad de producto como especialista y el responsable de seguridad de IT como coordinador.
2. El comité de seguridad debe tener por lo menos un integrante que sea C-Level para asegurar que la seguridad digital está presente en las decisiones estratégicas de la compañía.
3. Los cambios realizados por el comité de seguridad serán reflejados en este documento de forma anual, y han de ser aceptados por los trabajadores al entrar en la compañía y una vez al año a través del siguiente formulario.