cabify

Política de Protección de Datos y Ciberseguridad

Índice

1. Introducción

La presente Política de Protección de Datos y Ciberseguridad, liderada por el área de Stakeholder Relations y aprobada por C-Leve el día 30 de noviembre de 2023, tiene como objetivo establecer los principios, compromisos y el marco general de actuación que Cabify[1] asume para garantizar la protección de datos y la ciberseguridad. Cabify protegerá su información, de conformidad con la normativa aplicable y con sus valores éticos, definidos en el Código Ético, así como con lo previsto por el Comité de Dirección de la Seguridad de la Información.

El tener una Política unificada de Protección de Datos y Ciberseguridad persigue varios objetivos:

- Asegurar que los datos , tanto privados de la empresa (financieros, fiscales, propietarios, de ventas), como los datos privados de los clientes y personas que mantienen una relación profesional con Cabify, estén seguros ante posibles intentos de robo, copia o utilización inapropiada.

- Garantizar a clientes, inversores y colaboradores que el uso de datos dentro de la compañía cumple o excede los estándares de seguridad de una empresa moderna.

- Ofrecer a todas las personas que mantienen una relación profesional con Cabify las herramientas necesarias para que puedan realizar su trabajo 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 se basa la seguridad de los datos.

2. Ámbito de aplicación

La presente Política es de aplicación y obligado cumplimiento por la totalidad de la plantilla de Cabify y todas las personas que ejerzan cargos directivos en cualquiera de los territorios en los que Cabify esté presente.

3. Compromiso

Cabify asume el compromiso de adoptar las medidas de seguridad fundamentales para garantizar la integridad y privacidad de los datos.

[1] Se entiende por Cabify todas las sociedades que componen el Grupo Cabify.

La parte más importante de una Política de Protección de Datos y Ciberseguridad es su cumplimiento y la primera y más importante línea de defensa que tiene Cabify contra posibles intrusiones o intentos de robo de datos es su plantilla.

Consecuentemente, los principios de actuación, a continuación enunciados, son de obligado cumplimiento.

4. Principios de actuación

4.1. Medidas básicas de ciberseguridad

A continuación se hace mención a las medidas más básicas de seguridad que son comunes a todas las personas usuarias de Cabify. Estas medidas, aunque en muchos casos simples y evidentes, son la herramienta más importante que se tiene para evitar fugas de datos o intrusiones en los sistemas.

1. Las claves de todos los sistemas son personales e intransferibles, no deben ser compartidas con nadie, ni siquiera IT o jefe/supervisor. IT nunca te pedirá tu contraseña.

2. Todos los accesos a sistemas de Cabify están gestionados a través del SSO corporativo y con obligatoriedad de utilizar autenticación de doble factor. Los accesos “de servicio” a las plataformas tienen sus propias reglas de seguridad avanzadas que van varios pasos por encima de usuario/contraseña/MFA.

3. Cualquier acceso que no requiera MFA debe ser reportado al departamento de Seguridad de la información para que sea subsanado.

4. Es necesario bloquear el equipo al levantarse. De no hacerlo, una vez habilitado en el dispositivo, JumpCloud lo hará automáticamente.

5. Si se utiliza correo en el teléfono, es obligatorio PIN o patrón/huella. Si la terminal es de empresa, tendrá el MDM de google instalado. Si se pierde o es robado, debe reportarse a IT inmediatamente. Para tener el MDM habilitado en teléfonos personales (medida extra de seguridad contra robos, a nivel profesional y personal), se puede habilitar también pidiéndolo a través de los canales correspondientes.

6. Cada persona es responsable de lo que ocurra con la información que comparta digitalmente, a efectos laborales y legales. Esto significa que si comparte información con personas no autorizadas, las consecuencias de su uso serán responsabilidad de dicha persona.

7. Mucho cuidado con el Phishing si se desconoce al remitente de un correo electrónico, o no se espera el correo, nunca deben abrirse 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 través de los canales correspondientes.

8. Extremar cuidado a la hora de compartir permisos de documentos. No compartir fuera de la organización si no es un colaborador con quien haya firmado acuerdos NDA.

9. Nunca debe compartirse información de nombres de servidores, contraseñas o códigos en general en ningún foro público o privado en Internet.

10. No debe instalarse ninguna aplicación por API contra google sin consultar primero (esto significa que si te pide la cuenta de Cabify para conseguir acceso, debe usarse API). Se harán barridos periódicos de las aplicaciones conectadas por API, y se cortará lo que se desconoce... por lo que las aplicaciones no permitidas dejarán de funcionar.

4.2. Estándares de sistemas corporativos

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

1. Los equipos informáticos con los que se trabaja 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 más 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 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, el estándar de Cabify es Palo Alto Cortex XDR.

5. Todos los sistemas que trabajan en remoto deben tener disponible la VPN Prisma Access desplegada en sus equipos y activada cuando estén fuera de la oficina.

6. Todos los equipos informáticos de Cabify deben estar encriptados completamente. La encriptación será habilitada de forma remota y automática. Si un usuario descubre que por alguna razón su equipo no está encriptado ha de reportarlo inmediatamente a través de los canales correspondientes.

7. Trato del hardware de la empresa:

    a. Los usuarios son responsables del trato que den a los dispositivos de Cabify. 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 pudieran ser prevenidos (Ejemplo, se ha caído a la piscina).

    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 de la persona 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 el bloqueo de cuentas.

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. Éstas deben limitarse a transferencias de datos entre dispositivos internos de la compañía.

9. 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.

10. Las copias locales de datos deben ser la excepción, no la norma. La forma adecuada de trabajar en Cabify es en la nube, específicamente en Google Drive.

4.3. 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 del equipo de producto, es imperativo reportarlo de forma inmediata aquí. En caso de no tener acceso se debe contactar al manager correspondiente.
4. En caso de pérdida, robo o sospecha de problema de credenciales es imperativo reportarlo de forma inmediata aquí. En caso de no tener acceso, contactar con el manager correspondiente.
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.

4.4. 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 su plantilla. Es muy importante seguir 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 se seguirán unas normas básicas con el tratamiento de estos datos que garantizan que éstos 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 la plantilla.
2. Las personas que componen la plantilla 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 Cabify sin que antes haya firmado un documento donde certifique que se adhiere a la normativa vigente.
5. La plantilla debe abstenerse de enviar datos de carácter personal por correo electrónico salvo con consentimiento expreso de la persona cuyos datos están siendo compartidos.
6. Todos los datos en las carpetas compartidas de Cabify 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 Cabify serán borrados automáticamente sin previo aviso.
7. Cualquier persona con conocimientos de una fuga de datos, ya sean de carácter personal tanto de clientes como de personas pertenecientes a la plantilla, como propietarios y confidenciales de la empresa, ha de reportar esta fuga inmediatamente al correo electrónico dpo@cabify.com

5. Implementación

Para lograr una adecuada implementación y supervisión de la presente Política, Cabify ha establecido una estructura organizacional mediante la definición de roles sujetos a funciones y responsabilidades.

1. El C-Level tendrá la facultad indelegable de aprobar la presente Política y sus consecuentes revisiones anuales.
2. El Comité de Dirección de la Seguridad de la Información llevará a cabo la supervisión de la aplicación, el correcto funcionamiento y el cumplimiento de los principios y pautas establecidas en la presente Política.
    - Estará coordinado por el departamento de IT y el de producto, con la persona responsable de seguridad de producto como

especialista y el o la responsable de seguridad de IT como coordinador/a.

- Deberá 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.
- Se reunirá como mínimo una vez al trimestre, y tendrá un reporte del estado de la seguridad mensual distribuido.
- Reflejará los cambios realizados en este documento de forma anual, los cuales han de ser aceptados por la plantilla de Cabify al entrar en la compañía y una vez al año.

3. La totalidad de la plantilla es responsable de la correcta aplicación de los principios y controles enunciados en la presente Política, así como de identificar y denunciar cualquier posible caso de fraude o incumplimiento de normas regidas por la ética profesional.

Se realizarán revisiones de la presente Política de Protección de Datos y Ciberseguridad cuando se produzcan hechos relevantes que puedan afectar a su contenido.

cabify