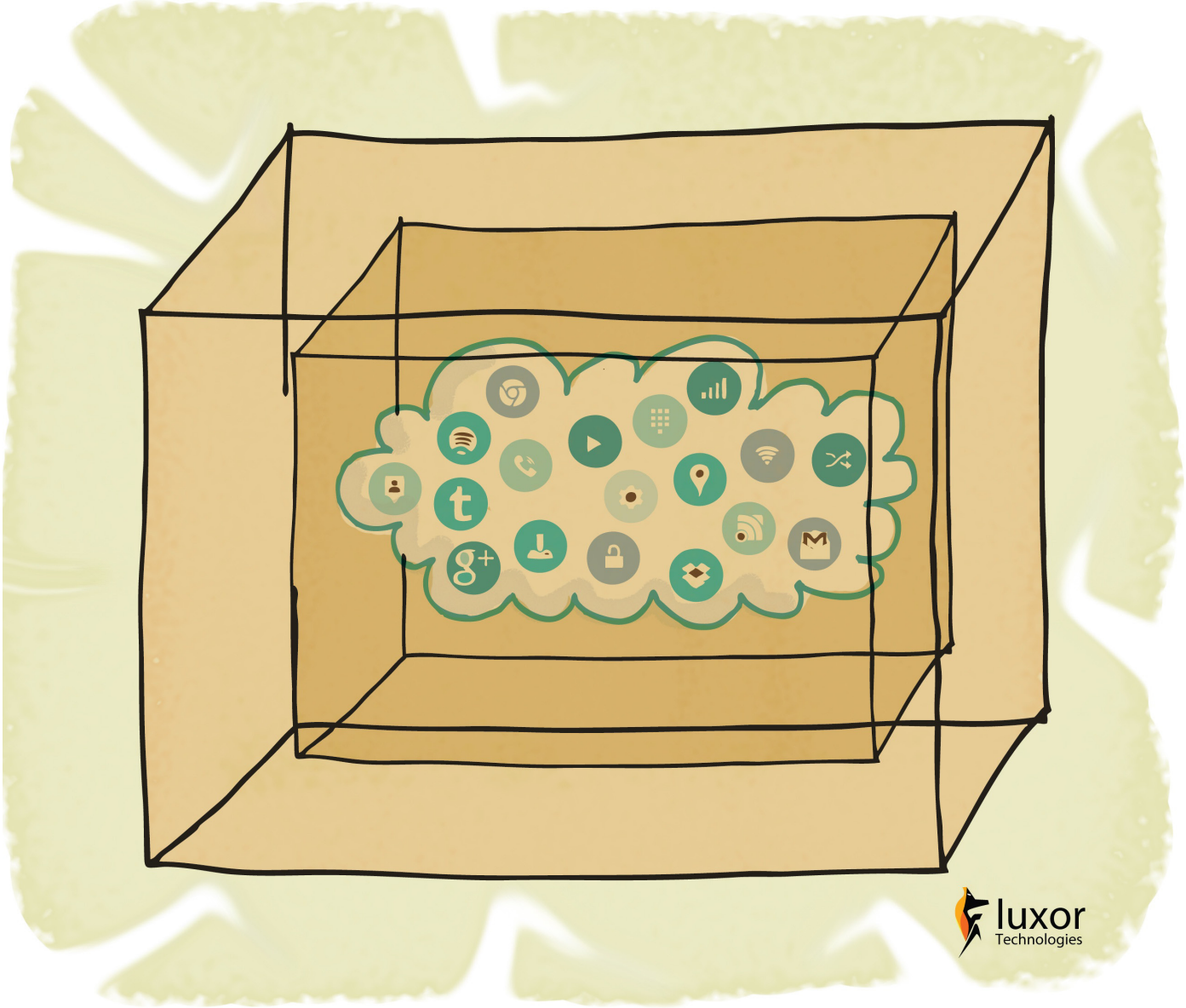


La nube segura

Uno de los factores más discutidos del cloud computing es la seguridad de la información volcada en los servidores. Los avances en las Telecomunicaciones ponen al día diversos controles rigurosos para acompañar el desarrollo de esta nueva filosofía laboral, tendencia para los próximos años. Múltiples compañías, proovedoras de los servidores, se actualizan de manera constante y ofrecen a sus clientes productos que se rigen por las últimas normas declaradas en la industria. Así, es conveniente repasar todas las recomendaciones pertinentes y las mejores prácticas que se deben considerar, acordes a la seguridad y a la confidencialidad de la información que se procesará en la nube. Existen siete elementos por los cuales se pueden desencadenar diversas amenazas que van en contra de una nube segura, pero que ya se ven disminuidas por la aplicación de estas recomedaciones.

A continuación, describiremos, dentro de cada uno de los siete elementos, las sugerencias para garantizar una nube segura.

Uso de la nube: el acceso público amenaza al servicio por la gran posibilidad de verse interferida por códigos maliciosos e información no deseada. Por lo que se sugiere:

1. Restringir el acceso al servicio.
2. Monitorizar la plataforma en tiempo real.
3. Monitorizar el tráfico de usuarios.
4. Brindar capacitaciones a los usuarios.

API: el control del servicio se realiza a través de múltiples interfaces. Por lo que se sugiere:

1. Conocer las interfaces utilizadas por los proveedores de los servidores que alojarán la nube de información.
2. Utilizar servidores que tengan API autenticadas.

Usuarios: aquellos que tengan acceso a la nube pueden provocar amenazas (con intención, si están descontentos con la compañía, por ejemplo). Esta amenaza es transversal a todo tipo de negocio y se ve atravesada por las relaciones laborales. Por lo que se sugiere:

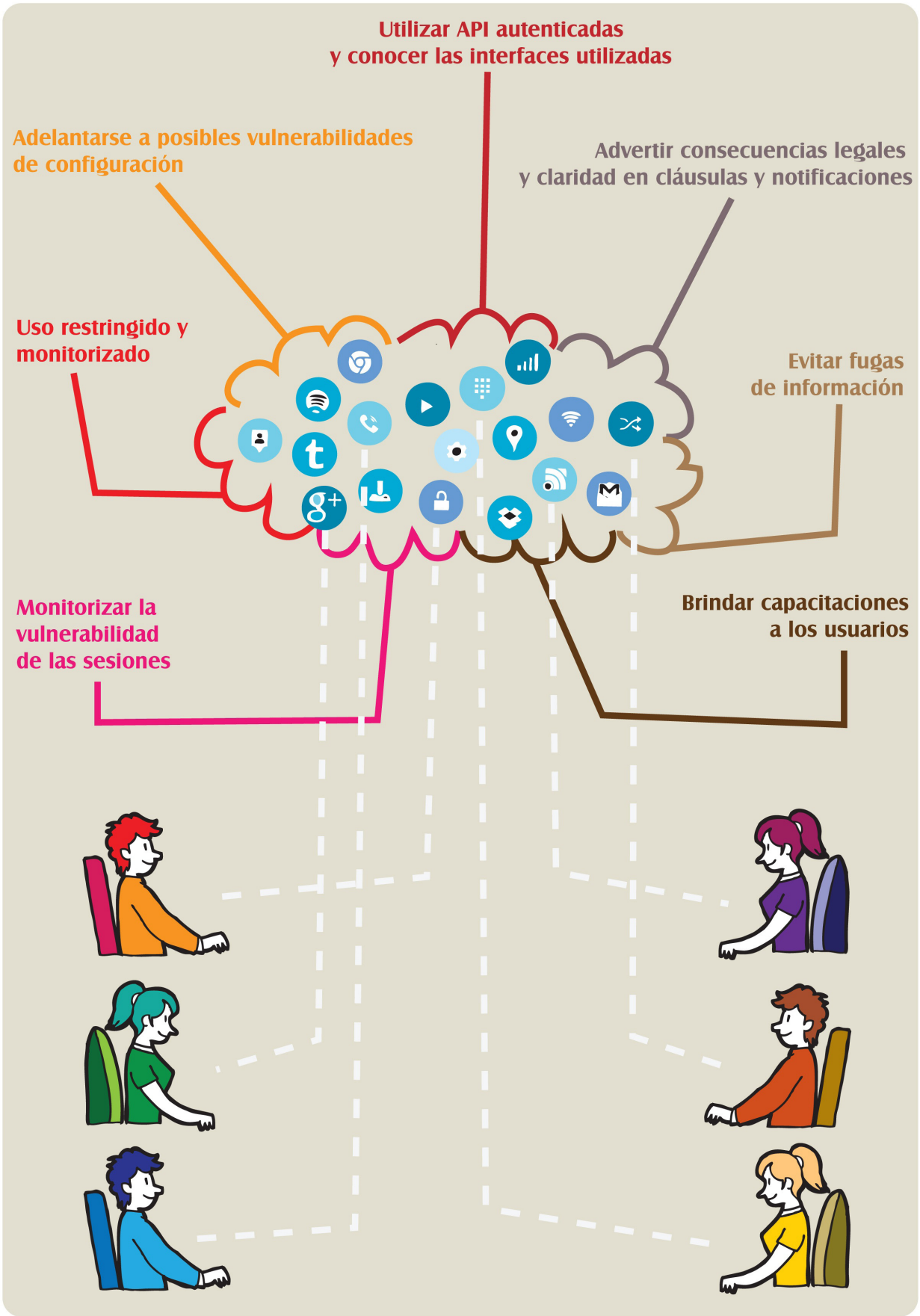
1. Advertir las consecuencias legales en los contratos laborales.
2. Especificar las cláusulas de confidencialidad en los contratos laborales.
3. Gestionar un plan de comunicación de procesos y procedimientos claro para la notificación de posibles problemas.

Tecnologías: compartir redes, recursos y utilidades amenaza a las infraestructuras compartidas cuando no tienen un claro control de los puntos en los que se realiza la conexión entre ellos. Por lo que se sugiere:

1. Establecer las mejores prácticas para la configuración de las infraestructuras.
2. Diseñar una correcta configuración de la plataforma.
3. Monitorizar el entorno de la plataforma en tiempo real.
4. Gestionar accesos diferenciados para los administradores de las infraestructuras.
5. Adelantarse a las vulnerabilidades posibles que puede acarrear cada elemento compartido.

Información: los datos volcados en la nube son diversos. Para asegurar su correcto procesamiento es importante evitar fugas y accionar un plan de contingencia adecuado. Por lo que se sugiere:

1. Controlar el manejo, a través de interfaces autenticadas y potentes.
2. Cifrar los datos.
3. Monitorizar el tráfico de la información gestionada.
4. Brindar servicios de control, a través de claves.
5. Generar mecanismos seguros para la destrucción de la información.
6. Definir las políticas de diseño, administración, gestión, procesamiento, archivo y destrucción de la información.



luxor Technologies

Sesiones: si la información de acceso es vulnerada, las sesiones se ven amenazadas. Por lo que se sugiere:

1. Establecer consecuencias legales en los contratos laborales para prohibir que se compartan los datos de acceso con terceros.
2. Aplicar accesos discriminados con múltiples mecanismos de control y de autenticación de usuarios.
3. Monitorizar la labor en tiempo real para observar de inmediato cualquier actividad inusual.

Capacitaciones: si no se conoce la base del funcionamiento de la nube, la gestión se ve amenazada por no contar con elementos que permitan tomar decisiones acertadas. Por lo que se sugiere:

1. Brindar capacitaciones a toda persona que acceda a la nube.
2. Actualizarse en la configuración de la plataforma.
3. Mantener un sistema de alerta vigente para la vigilancia de la información.
4. Monitorizar la actividad registrada en la infraestructura.

Una nube segura es posible, además, si se consideran algunos consejos sobre los riesgos posibles en la utilización de esta modalidad laboral, que admite el teletrabajo.

Entre las recomendaciones de los especialistas se destaca el acceso privilegiado a la información a aquellos usuarios que así lo precisen y el acceso restringido a aquellos usuarios que no requieran administrar la plataforma.

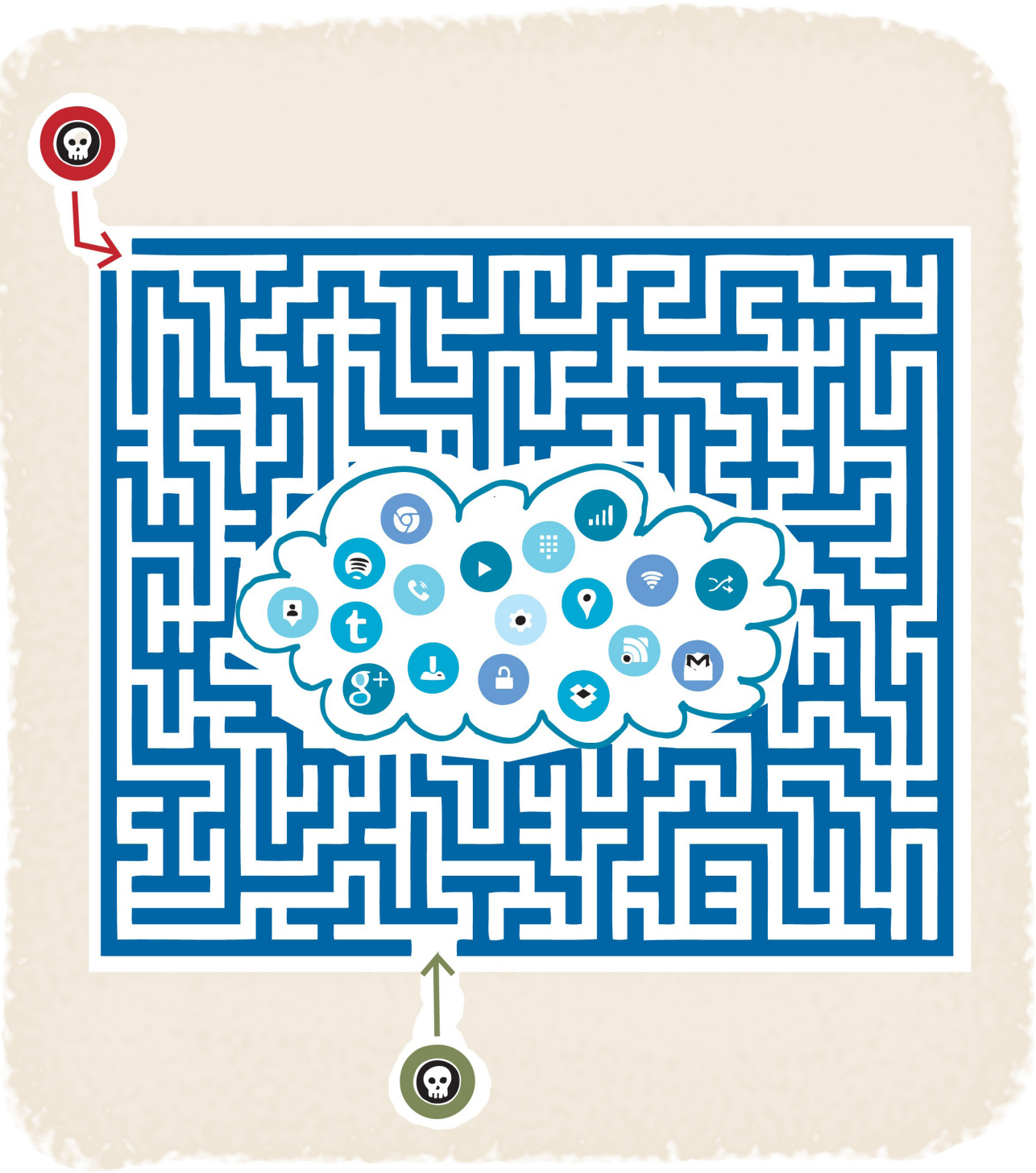
Por otra parte, las compañías deben volcar toda su información únicamente a proveedores que se presten a recibir auditorías constantes de calidad, que promuevan la protección de los datos, sobre todo de aquellos que son sensibles y que pueden poner en riesgo el negocio de la organización.
Para esto último se aconseja esclarecer el marco regulatorio en el que cada proveedor cabe según el servicio contratado.

El prestador del servidor debe garantizar, además, que la información contenida en la nube será cifrada y que ese procedimiento será gestionado por personal capacitado y competente.
Si la información sufriese alguna pérdida, el proveedor deberá garantizar su recupero y establecer el tiempo en que esta podrá volver a establecerse.

Por último, las compañías deben contemplar que su proveedor de servicios puede ser absorvido por otra compañía (a corto o a largo plazo). Esta es una realidad ajena a las organizaciones y una realidad que responde a los cambios que sufre de modo constante el mercado laboral, pero que debe ser advertida y que debe ser prevenida. Para esto es importante que en el momento de la contratación de un proveedor del servidor, en el cual se volcará toda la información corporativa, se establezca una cláusula que contemple esta posible realidad.

Así, se concluye que para contar con una nube segura es importante contar con políticas claras de acceso a la información, de provisión de servicios y desarrollar mecanismos de control de estas políticas.
Las regulaciones ya establecidas impactan sobre esta nueva modalidad y deben ser consideradas para el momento de la contratación de un proveedor del servicio de la nube.

Comprender las bases de acción de la nube permite una gestión controlada y segura de la información y una proyección sustentada de los objetivos corporativos que se desarrollarán mediante esta modalidad de trabajo en la nube.



¿Cómo podemos ayudarle?

Con nuestro software para callcenter: éxito en todas las llamadas, optimización de ventas, incremento de ahorros, orientación real de su trabajo a su core de negocio. Luxor Technologies desarrolló la plataforma más completa y avanzada que se integra a su auténtica necesidad. Podemos ayudarle. Contáctenos.

Dirección: Calle Diputació 238, Ático 1º. 08007 Barcelona

Tel. +34 935285252
Twitter: @luxortec
e-mail: info@luxortec.com

luxor Technologies