GRUPO garatu IT SOLUTIONS

Cómo proteger tu empresa

DESDE LA CIBERSEGURIDAD

GRUPO garatu IT SOLUTIONS

SYSTEMS & SECURITY · GARATUCLOUD.COM

Lo que debes saber sobre la seguridad informática de tu empresa para no perder el control

Desde sus inicios, las prácticas delictivas han ido superando barreras. Desde el spam masivo, hasta robos de credenciales, infecciones de los equipos, ataques de denegación de servicio o secuestro de PCs.

Otros perjuicios muy serios que pueden sufrir las empresas

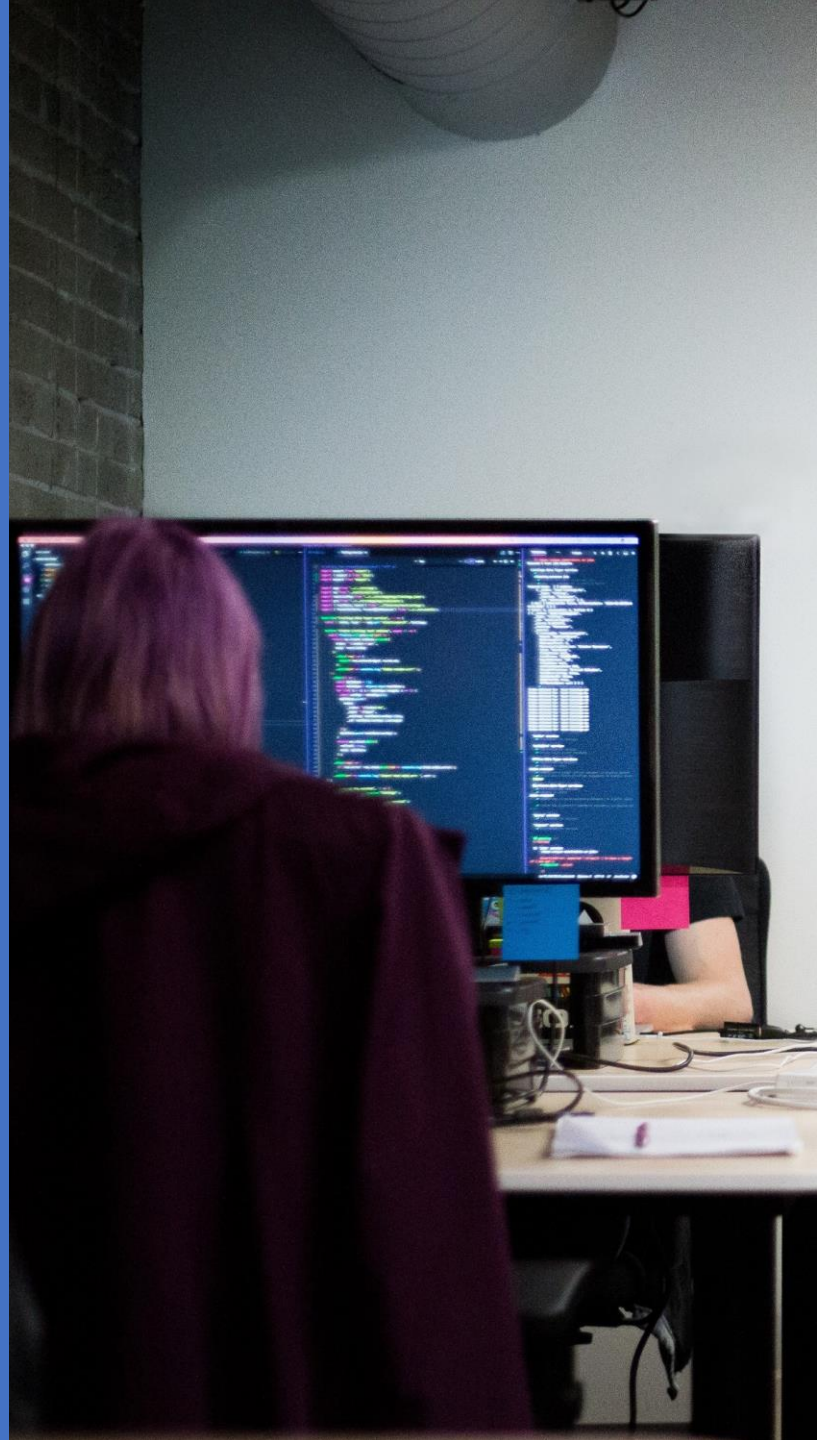
Sistemas bajo control del atacante, datos privados de clientes sacados a la luz pública, caídas de productividad, inactividad empresarial, sustitución en algunos casos de determinadas infraestructuras TIC, daños a la reputación e imagen de empresa, etc.

Por ello, necesitamos un

plan de seguridad efectivo

y enfocado específicamente a nuestra empresa.

info@grupogaratu.com · **+34 943 344 645**



¿Tu empresa está protegida? ¿Son efectivos los sistemas de seguridad actuales? ¿Debes de implementar nuevos métodos de seguridad?

La seguridad informática interna, externa y perimetral

1. **Seguridad interna**, que establece medidas de seguridad a nivel local dentro de la misma red para proteger los sistemas ante un atacante local e incluso ante las acciones, voluntarias o involuntarias, de los usuarios.
2. **Seguridad externa**, la cual integra elementos defensivos a todos los sistemas informáticos de la empresa para protegerlos frente a amenazas externas, procedentes en su mayoría de Internet.
3. **Seguridad perimetral**, que se define como los elementos y dispositivos electrónicos para la protección física de los sistemas.

Si preguntásemos a gente al azar sobre medidas de ciberseguridad, el antivirus y el firewall serían las dos más nombradas

1. El antivirus escanea -normalmente **en tiempo real**– todos los archivos y documentos que utilizamos en busca de amenazas como virus, malware, ***ransomware***, etc.
2. El firewall actúa de manera parecida, pero con la red, escaneando los paquetes que recibimos y enviamos, protegiéndonos de intrusos y otras amenazas.

Aunque dichas medidas sean muy útiles e imprescindibles, **en una empresa no son suficientes**.

Existen muchas otras medidas de seguridad, tanto internas como externas interesantes para completar con los antivirus y firewalls:

- **Sistemas de Detección y Prevención de Intrusos (IDS/IDPS).** Son dispositivos que monitorizan los sistemas de la empresa y generan alarmas si se detectan patrones de comportamiento sospechosos.
- **Honeypots.** Vulnerabilidades falsas puestas a propósito para recopilar información sobre los ataques a nuestra empresa.
- **Antispam.** Las medidas contra los correos no deseados son muy necesarias, pues actualmente el 80% de las amenazas de Internet llegan a los sistemas de la empresa a través del correo electrónico de los empleados
- **Redes Virtuales Privadas (VPN).** Túneles virtuales creados a través de la red para aislar y proteger comunicaciones.
- **Análisis y prevención de vulnerabilidades web.** En el caso de que tengamos alguna web App, también es importante protegerla frente a ataques.
- **Capa de punto final.** Medidas de seguridad que impiden la ejecución de programas y servicios sospechosos, restringen los privilegios y reducen la probabilidad de infección de los sistemas.

La Ciberseguridad en la empresa es un trabajo en equipo. Todos estáis implicados

Si diriges una empresa, debes de educar a tus empleados para que tomen conciencia de lo que son las **buenas prácticas en materia de seguridad.**

EN EL ESCRITORIO DE TU OFICINA

Bloquea siempre tu sesión en el pc que estés utilizando cuando abandones tu puesto.

TUS DISPOSITIVOS

Nunca instales aplicaciones que no sean oficiales
No conectes USB o Discos duros que no sean de total confianza
No modifiques la configuración y mantén actualizado tu dispositivo
Pon claves de acceso en todos ellos y la opción de bloqueo automático en todos tus dispositivos móviles

EQUIPOS PÚBLICOS

No te descargues en el pc de tu casa ficheros sensibles de tu compañía, incluso si has accedido a tu correo corporativo
Nunca utilices información sensible de tu empresa en equipos compartidos o públicos

PÉRDIDAS DE INFORMACIÓN RELEVANTE

Cualquier información sensible que tengas en papel, no la tires a la papelera. ¡Destrúyela!
Si mantienes una conferencia o una simple llamada de teléfono donde se manejan datos confidenciales, asegúrate de que nadie puede escucharte

GESTIÓN DE TUS CUENTAS CORPORATIVAS

Nunca apuntes tus contraseñas en papel. Memorízalas.
No compartas tus credenciales bajo ningún pretexto a ningún compañero
No uses las credenciales corporativas para páginas, servicios o aplicaciones personales

INTERNET

No accedas a páginas web que parezcan sospechosas.
Vigila que su url empiece por https
No clickes en links que no conozcas
No te descargues programas de los cuales no sabes su autoria
No abras ningún archivo .exe

CORREO ELECTRÓNICO

No abras ningún correo "raro": pago de una factura que no entiendes de donde viene, respuesta de alguien que no sabes quién es, premios otorgados, descuentos increíbles...

BACKUP DE LA INFORMACIÓN MÁS IMPORTANTE

Realiza Copias de Seguridad de la información más crítica que manejas y que solo esté en tus dispositivos
Piensa en pasarte a un Backup Online, pero fíjate que cumpla la normativa LOPD

CUIDADO CON TUS DESPLAZAMIENTOS

No lleves información crítica de tu compañía en dispositivos móviles a no ser que esté cifrada y tengamos todo el contenido codificado
No navegues a través de Wifis públicas manejando información corporativa

AVISA A TU DEPARTAMENTO

Ante cualquier duda o comportamiento extraño de tu dispositivo ponte en contacto con el departamento de seguridad de tu empresa

¿Qué es el RANSOMWARE?

La familia de Ransomware son virus informáticos que encriptan los datos del equipo infectado y otros equipos conectados en la misma red LAN. Exigen a la víctima realizar un pago para volver a habilitar el acceso al ordenador y a los datos.

Este tipo de amenazas normalmente entran en un fichero adjunto en un Email o descargado de una página Web y pueden tener apariencia de un documento legítimo como un programa o juego, un documento PDF, Excel o Word.

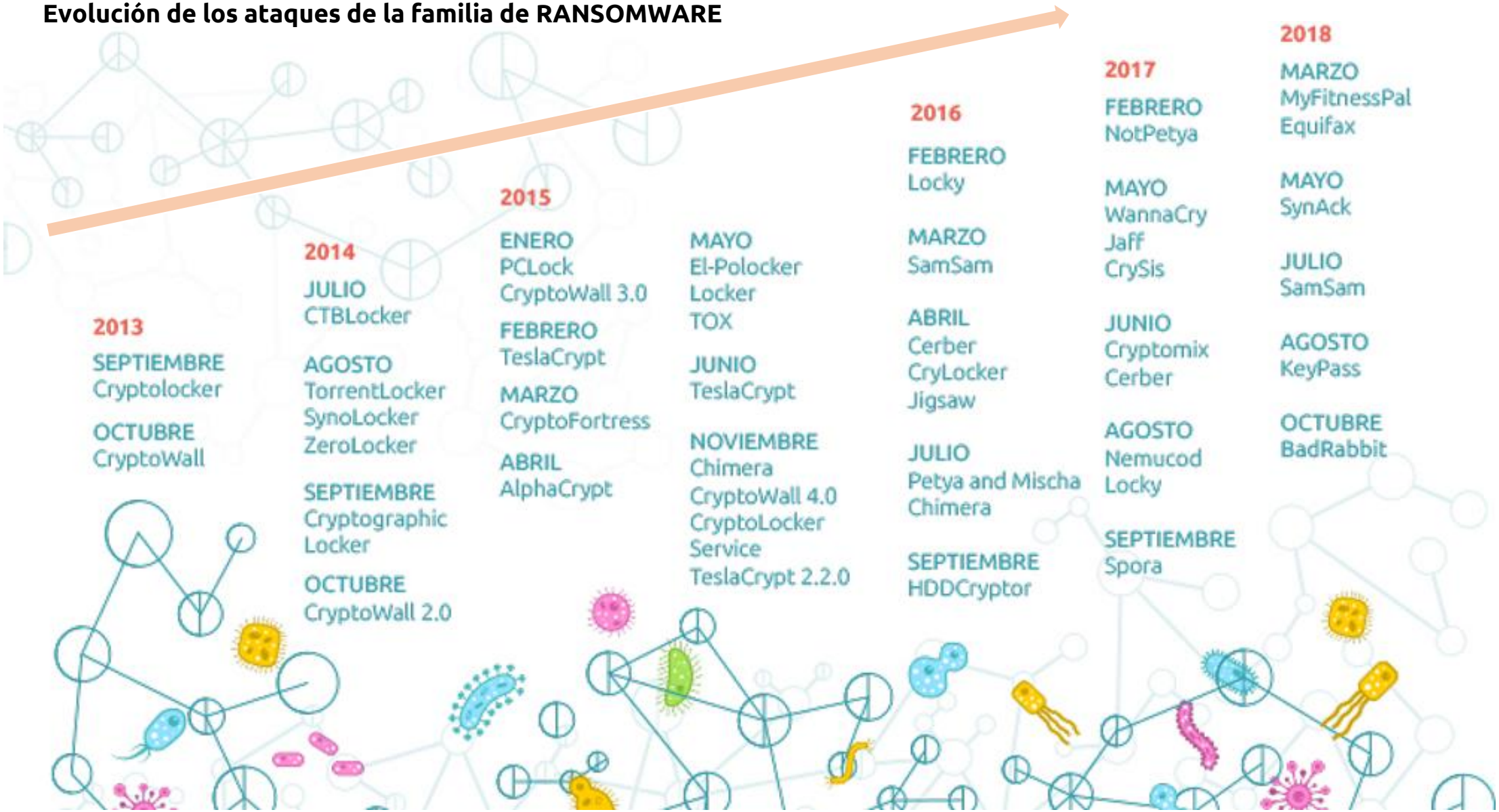
Las amenazas llegan mediante correos electrónicos, enlaces en las páginas Web, descargas de documentos con apariencia inocente, etc.

En la mayoría de los casos, cuando tu dispositivo ya está infectado y el malware ejecutado, hay que validar el tipo de virus y buscar la llave de descifrado.

La infección significa:

- Secuestro de tus datos con la consiguiente pérdida de los mismos si no se paga el rescate (muchas veces aunque se pague)
- Paralización de las operaciones de la empresa
- Gran perjuicio económico
- Daños en la reputación de tu negocio

Evolución de los ataques de la familia de RANSOMWARE



Buenas prácticas para evitar el RANSOMWARE y su familia de virus.

Prevenir los ataques es posible. Puedes evitar convertirte en una víctima de estos ciberdelincuentes siguiendo unos simples **consejos de seguridad**.

1.- EDUCANDO A LOS USUARIOS QUE TENGAS EN PLANTILLA

Antes de abrir un email

¿Conozco al remitente y es alguien en quien confío?. Cuidado al abrir un email. Podría estar infectado con Ransomware. Si no estás seguro de un adjunto, pregunta primero al remitente si te lo ha enviado.

¿El correo realmente viene de la dirección que parece? Comprueba que la dirección del remitente y no solo su nombre tenga sentido. Con frecuencia, adjuntos maquillados como recibos, facturas o justificantes son Ransomware.

En tu puesto de trabajo

Si el Antivirus de tu puesto alerta sobre algo, informa inmediatamente al responsable informático o al soporte técnico.

Buenas prácticas para evitar el RANSOMWARE y su familia de virus.

1.- EDUCANDO A LOS USUARIOS QUE TENGAS EN PLANTILLA

Navegando en Internet

1. Cierra todas las ventanas (popups) que solicitan actualizar información sobre una cuenta o instalar aplicaciones sin que lo hayas solicitado
2. Nunca hagas click en enlaces que advierten de que su ordenador está desprotegido, en peligro o que tiene un virus
3. Nunca haga click en enlaces que indican que has ganado un premio (¡si fuese el caso te informarían por otros medios!)

Una forma efectiva de **asegurar que los sitios web** que visitamos con frecuencia **son los que pensamos** es guardarlos como bookmarks. Así evitamos escribir mal la dirección del sitio y entrar en posibles páginas peligrosas. Se emplean sitios como “gogle.com” para contenidos maliciosos por tener un nombre casi igual a un sitio conocido.

Buenas prácticas para evitar el RANSOMWARE y su familia de virus.

2.- PREPARA LA INFRAESTRUCTURA NECESARIA

Copias de seguridad

Asegúrate que se realiza el backup con frecuencia de todos los datos importantes, preferiblemente tanto en local como en un servicio Cloud. Realizar el backup únicamente en un disco externo lo pone en riesgo de que sea encriptado por un Ransomware de la misma forma que otros datos de los equipos.

Mantén actualizados todos los equipos

Es importante mantener al día con parches del sistema operativo y de los programas instalados tanto los PCs como los servidores.

Seguridad Perimetral y End-Point

Todos los equipos y servidores deben tener un Antivirus de calidad con análisis de comportamiento y servicios de reputación instalado y actualizado.

Un Firewall tipo UTM o Next Generation Firewall debe tener activados y correctamente configurados los servicios como IPS (sistema de prevención de intrusos), filtrado de URLs, antivirus o antispam.

Buenas prácticas para evitar el RANSOMWARE y su familia de virus.

2.- PREPARA LA INFRAESTRUCTURA NECESARIA

Plan de Continuidad de Negocio – BRS fácil

BRS Fácil es un servicio de contingencia para la continuidad del negocio que te permite seguir trabajando con las aplicaciones más críticas cuando los servidores de la empresa no están disponibles (por averías en Hardware, caídas de red, inundaciones, incendios, robos…).

Servicio Gestionado

Externalizar la seguridad de la infraestructura informática de su empresa incluyendo mantenimiento, monitorización, gestión de garantías, de inventariado y de licencias te asegura que un equipo de expertos lleve a cabo todas estas pautas que te hemos recomendado.

Si piensas que puedes estar infectado,

¡NO PAGUES A LOS HACKERS!

Pagar no te garantiza el rescate de tu pc, dispositivos móviles o archivos.

Desconecte el equipo de la red y llame a su proveedor de servicios de TI inmediatamente

https://noransom.kaspersky.com/es/

En esta web actualiza los listados de herramientas con las que podrías recuperar tus datos, **aunque no siempre es posible**

GRUPO garatu IT SOLUTIONS

SYSTEMS & SECURITY · GARATUCLOUD.COM

OBJETIVO PHISHING FRAUDE

1. Instala un antivirus con antiphishing
2. Verifica que su ordenador esté libre de cualquier tipo de malware
3. Verifica la fuente de la información cuando recibas un correo
4. Nunca contestar automáticamente a ningún correo que te pida información personal
5. Si te envían a una web, verifica que es una dirección segura.
6. Si tienes dudas de la veracidad del mensaje o de su procedencia, contacta por otro medio
7. Desconfía de las url acortadas,
8. No descargues ningún archivo .exe
9. No realices una transacción sin verificar la seguridad de la web y la 'Pasarela de pagos'
10. Si sospechas que fue víctima del Phishing, cambie inmediatamente todas sus contraseñas y póngase en contacto con la empresa o entidad financiera

Objetivo Phishing: luchando contra el fraude

El Phishing es uno de los métodos más utilizados por los ciberdelincuentes.

El ataque comienza enviando a la víctima un correo electrónico, suplantando a una fuente conocida –red social, tienda online, banco, institución pública, etc. -con el objetivo de robarte información privada.

En ese email te piden que descargues un archivo, hagas clic en un enlace que te enviará a una página falsa o te piden directamente en el mismo correo los datos confidenciales objetando algún motivo impostergable.

¡Ojo! Porque son muy ocurrentes y emplean tácticas muy ingeniosas:

- Nueva detección de estafa y apremiante actuación de seguridad.
- Novedosos consejos de seguridad para bloqueo del fraude.
- Simuladas ofertas de empleo.
- Movimientos o entradas sospechosas a tu cuenta.
- Cambios en la política de seguridad de la entidad.
- Ingresos económicos repentinos.
- Premios, regalos con poco margen de tiempo para que los aceptes.
- Inminente cancelación del servicio.

info@grupogaratu.com · +34 943 344 645

Gestión de contraseñas

Este es, sin duda, **el error más común** que se cometen en las empresas en temas de ciberseguridad.

Si con las claves que utilizamos para nuestras cuentas personales ya **hay que tomar ciertas precauciones**, con las que dan acceso a la información de nuestra empresa mucho más.

Para ello, debemos seguir las recomendaciones habituales para crear una buena contraseña:

- Evitar que contenga información personal sobre nosotros.
- No usar la misma clave en diferentes lugares.
- Que contenga números, símbolos y letras, todo ello mediante una combinación de mayúsculas y minúsculas

Por otro lado **debemos evitar a toda costa el más que conocido post-it pegado en la pantalla del ordenador** o situaciones homólogas a ello e igual de irresponsables.

Finalmente, nunca debemos revelar nuestra contraseña a alguien que la solicita por teléfono o correo electrónico. Bajo ningún concepto.

GRUPO garatu IT SOLUTIONS

SYSTEMS & SECURITY · GARATUCLOUD.COM