Seguridad en el teletrabajo

mrHouston
TECH SOLUTIONS

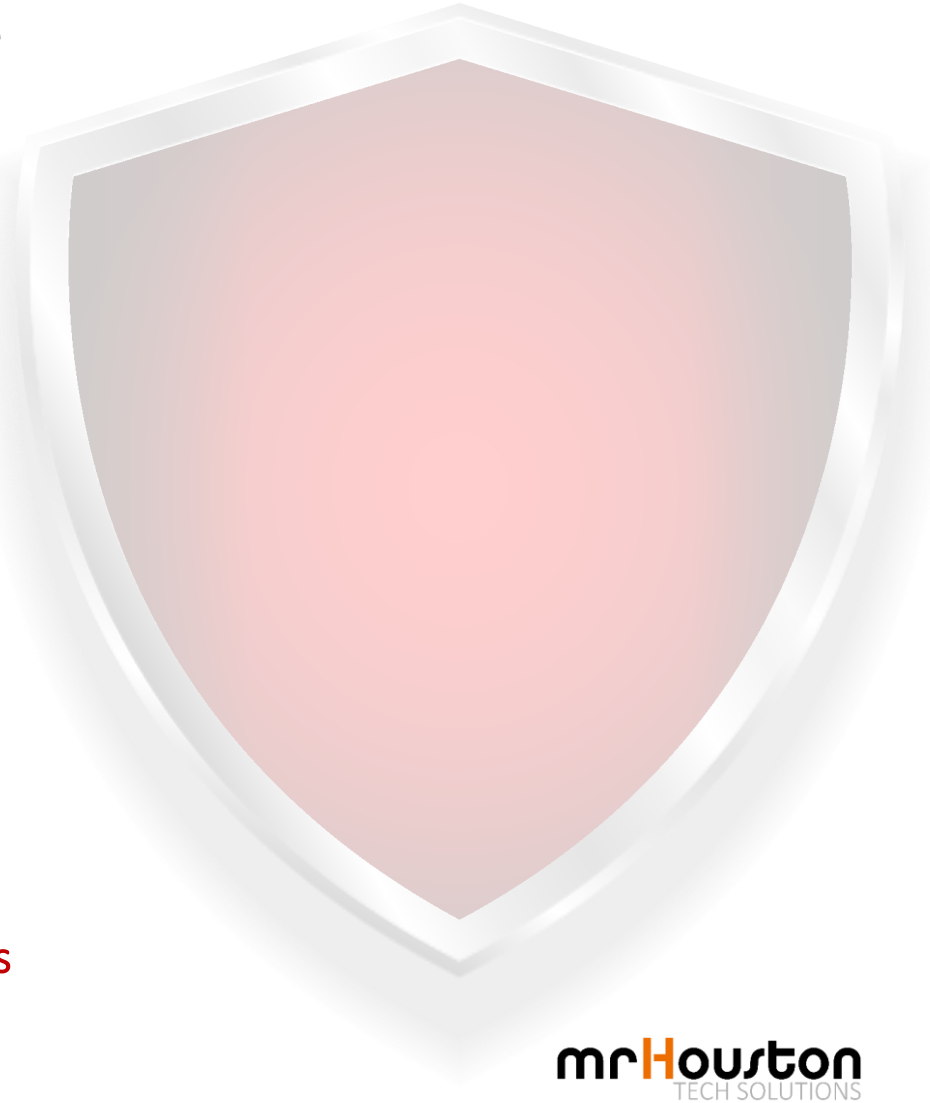
contexto

- Aunque es la primera vez que nos enfrentamos a una pandemia, es sabido que en **momentos de crisis:** sanitarias, desastres naturales, medioambientales o de otra índole, suele producirse un **aumento exponencial de ciberataques**, tanto a particulares como a organismos oficiales y empresas.

- Para las empresas, el **teletrabajo repentino** supone un **mayor riesgo** de sufrir **brechas de seguridad**, al no tener los protocolos necesarios implementados de antemano y ser más laxos en materia de ciberseguridad.

- Esta modalidad de trabajo supone un **cambio de paradigma** para la mayoría de nosotros que nunca hemos teletrabajado de forma tan continuada, ya que existe una **falta de hábitos y de medios** para poder llevarlo a cabo correctamente.

- Además, estar en casa a resguardo estos días puede provocar una **falsa sensación de seguridad**. Todos podemos ser un riesgo para la empresa en materia de ciberseguridad. Desde el CEO hasta el becario, **todos representamos una vulnerabilidad potencial** en la cadena.



mrHouston TECH SOLUTIONS

exposición a riesgos

TECNOLÓGICOS

Entendidos como aquellos derivados de la actividad de la propia empresa:

- ✓ Phishing.
- ✓ Ransomware.
- ✓ Políticas de BYOD (Trae tu propio dispositivo).
- ✓ Seguridad en la nube.
- ✓ Brechas en proveedores y colaboradores.
- ✓ Falta de concienciación.

GOBERNABILIDAD, RIESGO Y CUMPLIMIENTO

Aquellos que vienen dados por el ecosistema externo de la empresa:

- ✓ Cumplimiento normativo.
- ✓ Riesgos de proveedores y colaboradores.
- ✓ Gestión de riesgos en la cadena de suministro.
- ✓ Suplantación de identidad.
- ✓ Reputación y marca.

concienciación

mrHouston
TECH SOLUTIONS

concienciación

- Es muy importante que estemos **todos concienciados** de que existe un mayor riesgo durante situaciones de emergencia, ya que los ciberdelincuentes aprovechan la **necesidad de información** de la población y la **sensibilidad** que una crisis de gran alcance provoca.

- Algunos ejemplos son las **ciberestafas**, **suplantaciones de identidad** o **peticiones falsas de donaciones**.

Para evitar estos ataques, una sencilla medida que nos puede ayudar es revisar muy bien los emails: el remitente, el contenido, las URLs y en especial estar alertas si nos urgen a actuar o nos alertan con cualquier excusa.

mrHouston TECH SOLUTIONS

riesgos y medidas

mrHouston
TECH SOLUTIONS

riesgos y medidas

SUPLANTACIÓN DE IDENTIDAD

- ✓ Consiste en **hacerse pasar por otra persona o entidad** con diversos objetivos: cometer algún tipo de fraude, obtener datos de manera ilegal, ciberbullying, etc.
- ✓ Por ejemplo: hacerse pasar por el servicio técnico para pedirte tus claves, utilizando **técnicas de ingeniería social**.

Utilizar contraseñas fuertes y doble factor de autenticación, no facilitar información sensible a terceros y asegurarnos de que la URL que visitemos empieza por *https:,* nos puede ayudar a impedir que obtengan nuestras claves de correo personal, cuentas bancarias, etc.

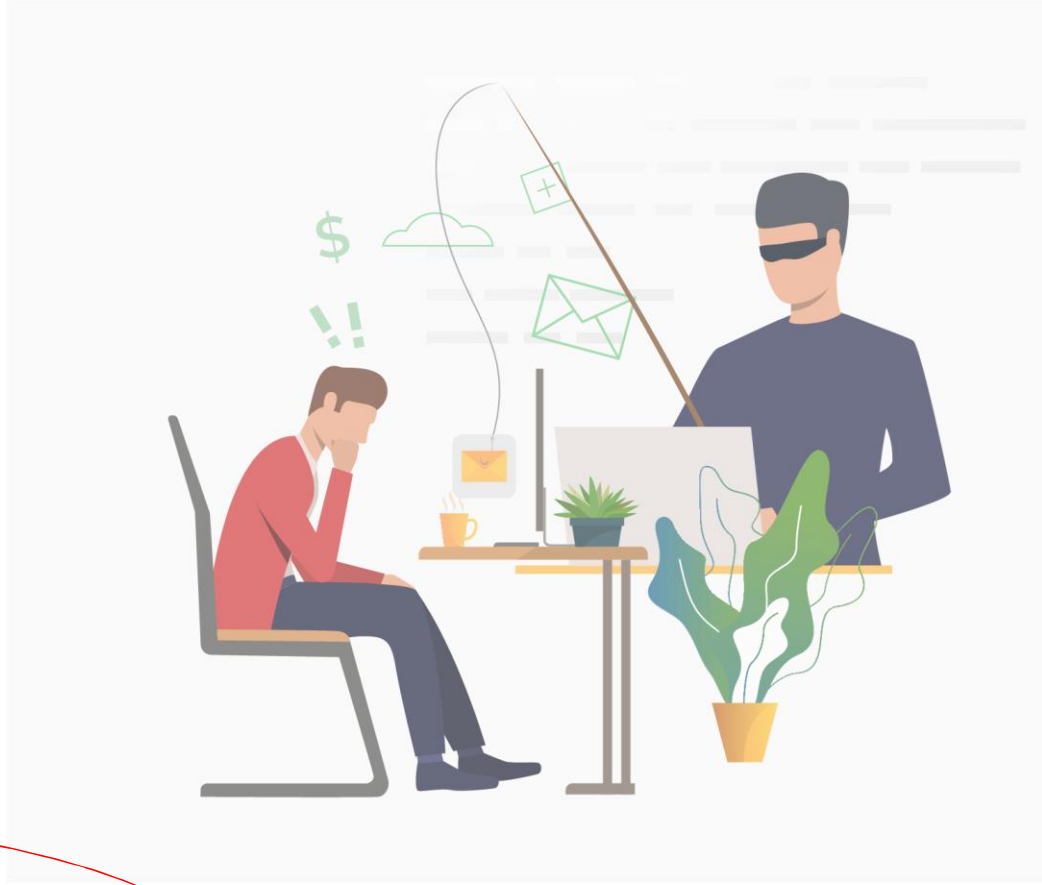
mrHouston TECH SOLUTIONS

riesgos y medidas

PHISHING

- ✓ Es una forma de **fraude** en la que el atacante intenta obtener las **credenciales** (usuario y contraseña) haciéndose pasar por una entidad, organismo oficial o persona de confianza a través del **correo electrónico u otros canales** (incluso por sms: smishing).

- ✓ Bastaría con enviar un correo "aparentemente" corporativo e incluir un enlace a un **sitio web suplantado** o a un **documento infectado** (por ejemplo, un protocolo de actuación frente a una crisis).



Para prevenir ataques de phishing deberíamos verificar las direcciones de correo de los remitentes, no abrir documentos o enlaces que no esperábamos recibir, y sobre todo usar el doble factor de autenticación para las cuentas de acceso.

riesgos y medidas

EQUIPOS NO PROTEGIDOS Y MALWARES

- ✓ Al trabajar con **equipos no protegidos,** ya sean **corporativos** o **particulares**, existe un mayor riesgo de ser infectado por **malware** (software malicioso).

Todos los equipos con acceso a información, aplicativos o recursos de la compañía, deben tener un nivel mínimo de protección. Una ventaja es tener sistemas licenciados por usuario y no por dispositivo. Esto permitirá que un mismo usuario pueda utilizar varios dispositivos de forma segura, económica y sin que perdamos el control de la seguridad global de la empresa.

riesgos y medidas

RIESGOS EN INFRAESTRUCTURAS

- ✓ Existen **tres formas principales** de llevar a cabo el **teletrabajo**:
  - ❖ Mediante **VPN** (Virtual Private Network) o red privada virtual.
  - ❖ **Conexiones remotas** y **sistemas desktop virtualizados**.
  - ❖ Conexiones a sistemas en la **nube (AWS, Azure, etc.)**.
- ✓ Con estos sistemas, dos de los riesgos principales son la **denegación de servicio**, lo que provocaría la imposibilidad de teletrabajar, y por otro lado que consigan **credenciales de acceso**.
- ✓ Con conexión remota, se añade el problema de seguridad de la propia herramienta utilizada para ello.
- ✓ Problemas con las **líneas de internet corporativas**.
- ✓ **Indisponibilidad de ancho de banda** suficiente en muchos casos.

riesgos y medidas

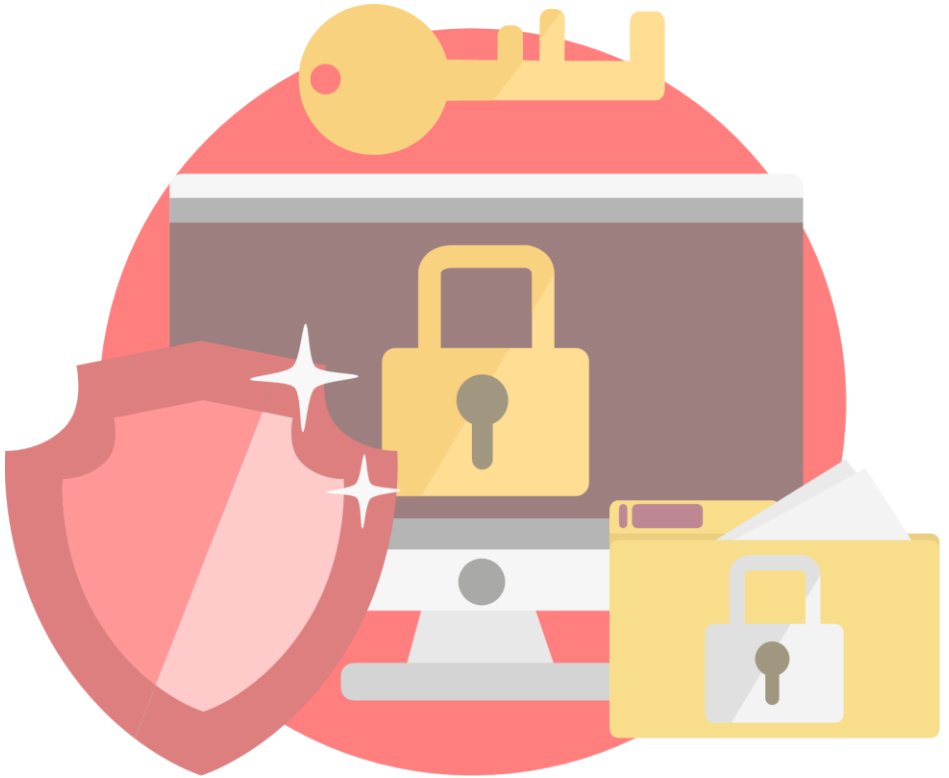
Algunas medidas para la seguridad en infraestructuras:

- Cifrado de datos sensibles de la empresa.
- Implementar medidas de seguridad de la red: firewalls de nueva generación, routers y switches actualizados, etc.
- Implantar medidas de prevención de pérdida de datos (DLP), orientadas también a la monitorización y control.
- Introducir sistemas de detección y prevención de intrusos, que frenen accesos no autorizados, como sistemas IPS (Intrusion Prevention System) o NAC (Network Access Control).
- Realizar copias de seguridad y pruebas de restauración periódicamente.

riesgos y medidas

RIESGOS PARA LA INFORMACIÓN

- ✓ La **seguridad de la información** asegura la **confidencialidad**, la **disponibilidad** y la integr**idad de los datos**, haciendo frente a los riesgos, analizándolos y previéndolos.



Algunas medidas para asegurar nuestros datos son:

- Cifrado de la información, los soportes que la almacenan y las comunicaciones (información en tránsito).
- Realizar copias de seguridad periódicamente y en varias ubicaciones (local y cloud).
- Utilizar contraseñas robustas y doble factor de autenticación.
- Controlar el acceso de los usuarios a la información.

riesgos y medidas

ATAJOS

- ✓ Cuando las **empresas** adoptan apresuradamente servicios de **SaaS** (*Software as a Service*), sin valorar las consecuencias o sin tener en cuenta posibles **problemas de seguridad**, están exponiendo sus sistemas y usuarios.

- ✓ Un **usuario** que no cuenta con las **herramientas adecuadas** para **teletrabajar**, a veces tiene que **buscar soluciones** para llevar a cabo su trabajo (por ejemplo: compartir información), y puede recurrir a herramientas que son **inseguras** o que su mera descarga desde la web, supone un serio riesgo para la seguridad de la empresa.

La empresa debe estar preparada para que los empleados utilicen las mismas herramientas de trabajo dentro y fuera de la oficina. Se debe formar adecuadamente a todos los empleados y recordar que la concienciación es crítica.

mrHouston TECH SOLUTIONS

riesgos y medidas

RIESGOS ANTE EL USO DE DISPOSITIVOS MÓVILES

- ✓ Los riesgos vienen dados, generalmente, por el **comportamiento o despiste del usuario**: descarga de aplicaciones maliciosas, acceso a sitios no autorizados, pérdida del dispositivo, etc.

Para aumentar la seguridad de los dispositivos móviles recomendamos:

- Creación de contenedores cifrados y gestionados por la empresa (Bring Your Own Device).
- Gestión de los dispositivos corporativos por parte de la empresa para controlar el uso y contenido del dispositivo.
- Implementar sistemas de autenticación de múltiple factor.
- Cifrado de las comunicaciones de datos.

mrHouston TECH SOLUTIONS

resumen

mrHouston
TECH SOLUTIONS

resumen

- ✓ Ante situaciones de crisis, **aumentan los ataques** y los **riesgos** a los que nos vemos expuestos todos a nivel de **ciberseguridad**.
- ✓ En una empresa **todos** debemos estar **concienciados**. Cada empleado es una brecha potencial. La **dirección** es **objetivo principal** por su mayor acceso a información y por poder autorizar pagos o transferencias.
- ✓ Las empresas deben dotar de **medios, herramientas y formación adecuados** para el teletrabajo. La **concienciación** es **clave**.
- ✓ Los **ciberdelincuentes** suplantan identidades y **se interponen entre emisores y receptores de fondos** para desviar el capital. Es **crítico ser rápidos** en denunciar.
- ✓ Contar con un **colaborador tecnológico de confianza** nos permitirá establecer **protocolos de ciberseguridad** y **procedimientos adecuados** para el teletrabajo.

mrHouston TECH SOLUTIONS

+34 - 91 432 02 86
soluciones@mrhouston.net
www.mrhouston.net