mrHouston
DATA&TECHSOLUTIONS

#ConsejosmrHouston

Guía de ciberseguridad para empresas

info@mrhouston.net

¿QUÉ CONTIENE ESTE E-BOOK?

CONTEXTO

Hoy en día, el mundo virtual es un mar de peligros si no sabes moverte con seguridad. Es por eso que es muy importante conocer los riesgos a los que te expones.

Algunos de las amenazas más frecuentes son:

Phishing: esa forma de fraude en la que el atacante intenta obtener información particular haciéndose pasar por una entidad o persona de confianza a través del correo electrónico u otros canales.

Scam: engaños o estafas de internet que pueden llegar a través de spam o técnicas de ingeniería social. Buscan acceder a tu información personal convenciendo al usuario de la prestación de un servicio.

Ransomware: programa informático malintencionado que infecta el sistema y restringe accesos a archivos y partes afectadas. Se pide un rescate a cambio de quitar esta restricción.

Robo de información: la información, sin precaución, puede ser siempre interceptada por terceros, que suele ir enfocada al robo de datos personales o fuga de información.

La **concienciación** y **formación** en materia de ciberseguridad es esencial. Los datos son el nuevo objetivo de los ciber-delincuentes. Poniendo en práctica las medidas de esta guía tu empresa estará mucho más segura.

mrHouston®
DATA&TECHSOLUTIONS

159,700

Ciberataques dirigidos a negocios en España durante el año 2017.

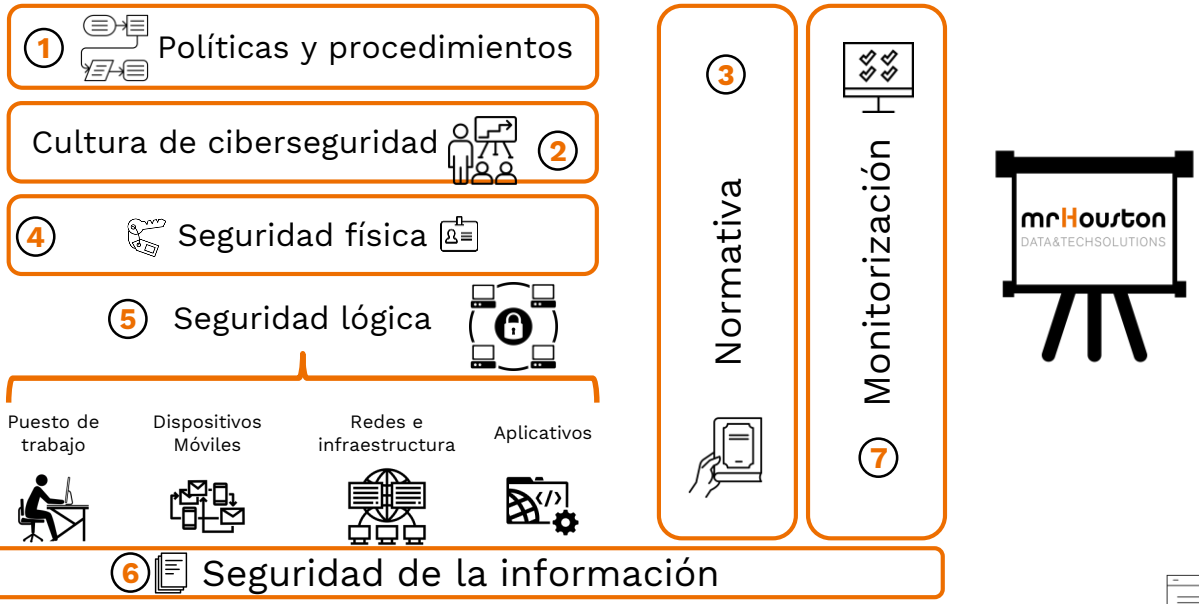
En 2016, la cifra se situó en

82,000

Pincha en cada sección para acceder a ella

¿QUÉ VAS A ENCONTRAR?

La seguridad en una empresa empieza desde su puerta. Por eso es necesario controlar desde la seguridad física hasta la monitorización de la infraestructura, equipos de usuarios y establecimiento de protocolos.
Te ayudamos, con esta guía, a establecer una **seguridad integrada** en tu empresa.



1 POLÍTICAS Y PROCEDIMIENTOS (I)

Tratan de planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la empresa.

Las políticas de seguridad se dividen en:

Prevención – Para un buen control de seguridad, algunas medidas son:

- Control de acceso
- Identificación y autenticación
- Seguridad en las comunicaciones

Detección

•Detectar las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema.

Recuperación

- Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento.

1

POLÍTICAS Y PROCEDIMIENTOS (II)

Y deben ...

Definir:
- Qué es seguridad de la información
- Sus objetivos
- Importancia en la empresa

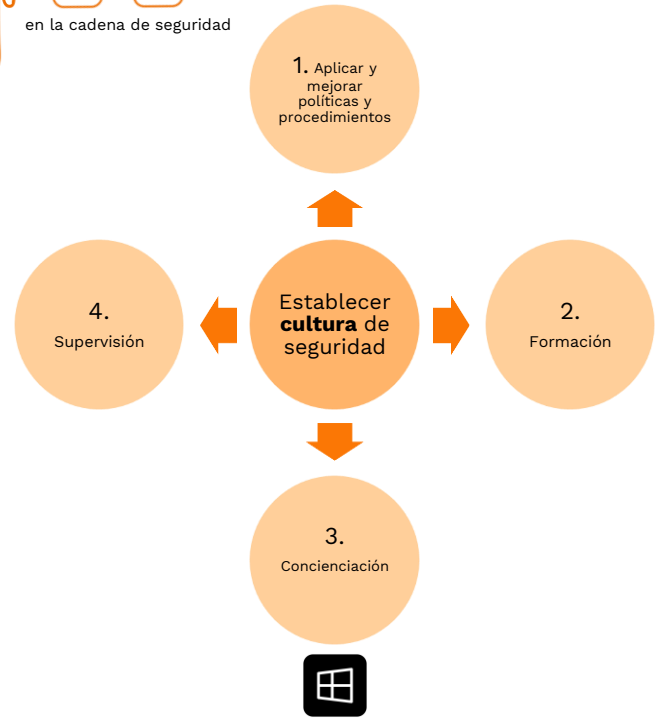
Mostrar compromiso
- Desde la dirección
- Estableciendo responsabilidades

Diseñar normas y procedimientos internos como:

1. Normativa de uso de dispositivos BYOD, e-mail corporativo, etc.
2. Medidas de carácter técnico como política de contraseñas
3. Prohibición de publicar o compartir contraseñas
4. Obligación de bloquear la sesión al ausentarse del puesto
5. Usar adecuadamente medios de almacenamiento extraíbles
6. Obligación de notificar cualquier incidente

2

CULTURA DE CIBERSEGURIDAD



Acciones de formación

Conceptos básicos sobre seguridad informática (qué es phishing, ransomware, etc.), herramientas y buenos usos.

Sobre cómo aplicar los controles de **seguridad física**: accesos autorizados, acompañamiento de las visitas, etc.

Protección adecuada del equipo personal: bloqueo al ausentarse, disponer de antivirus, realizar actualizaciones siguiendo los protocolos...

Sobre los **riesgos** que entraña acceder a webs peligrosas, aplicaciones no validadas por el departamento de informática o ejecutar archivos externos.

Cómo mantener a salvo los **dispositivos móviles**, tanto smartphones como portátiles o tablets.

Métodos para reconocer ataques de **ingeniería social** y para evitarlos.

Acciones concienciación

Se debe realizar una concienciación constante mediante acciones divulgativas y píldoras de información.
En primer lugar, informar sobre la gran **importancia del usuario** en la cadena de seguridad de la empresa, consiguiendo la implicación de todos los empleados, incluida la dirección.

Directivos	Managers	Equipo
•Seguridad de la información •Cumplimiento legal •Identificación y gestión de riesgos •Desarrollo de estrategias de seguridad	•Clasificación de la información •Fuga de información •Uso correcto de los medios •Incidentes de seguridad y su gestión	•Introducción a la seguridad •Buenas prácticas en puesto de trabajo •Gestión de incidencias •Cumplimiento normativo

Supervisión

El **responsable de seguridad** se encargará de:

Mantener la **vigencia y actualización** de políticas y procedimientos, detectando los posibles cambios que se produzcan en el entorno.

Realizar la **implantación** y velar por el **cumplimiento** de los procedimientos y las normas.

Asegurar que se realicen las correspondientes **auditorías**, internas o externas y asesorar acerca del impacto y consideración del riesgo.

Utilizar herramientas de **monitorización** para hacer análisis del uso de recursos.

Informar a los empleados de los métodos de monitorización manejados por la empresa.

3

Para más información sobre GDPR, consulta aquí nuestros artículos.

NORMATIVA (I)

RGPD / GDPR

- Regulación general de protección de datos.
- Sus objetivos:
  - Dar al ciudadano mayor control sobre sus datos.
  - Unificar la legislación respecto al tratamiento de datos a nivel europeo.
  - Promover el cambio tecnológico entre las empresas.

¿A quién y cómo afecta?

- Aplica sobre cualquier empresa que opere en la UE.
- Las organizaciones tendrán que demostrar que cumplen con la RGPD.
- Obligación tener un Delegado de Protección de Datos*.
- Obligación de notificar a las Agencias de Protección de datos de las brechas de seguridad.

*Para grandes empresas, administraciones públicas y empresas que manejen datos muy sensibles.

Medidas de adaptación

- Prevención de ataques externos (UTM, firewalls...)
- Prevención ante la fuga de información.
- Comunicaciones seguras mediante control de acceso, WIFI segura...
- Realizar auditorías de sistemas.

3

NORMATIVA (II)

LOPD

- Ley orgánica de protección de datos.
- Su objetivo es proteger los datos de carácter personal tratados en las empresas, ya sea de clientes o de empleados.

¿En qué afecta?

- Afecta a la seguridad de los datos personales gestionados por las empresas.
- Obliga a las empresas a notificar a la Agencia Española de Protección de Datos el tipo de datos que tratan.

Medidas de adaptación

- Obtener consentimiento de los afectados para tratar sus datos.
- Definir los ficheros a declarar.
- Precisar las medidas de seguridad aplicadas a los datos e implantarlas.
- Hacer documentos de seguridad.

3

NORMATIVA (III)

LSSI

- Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Su objetivo es proteger los derechos de los consumidores de servicios online.

¿A quién afecta?

- Proveedores de servicios de internet, alojamiento de datos y buscadores.
-Empresas y ciudadanos que utilicen internet con fines comerciales.

Medidas de adaptación

- Cumplir la LOPD
- Incluir información de empresa en la web o tienda online (denominación social, NIF, domicilio, e-mail, inscripción registral)
- Si se venden productos, incluir sus precios, impuestos y gastos de envío.

4

SEGURIDAD FÍSICA

¿Qué es?

Barreras y procedimientos para el control de las amenazas que pueda llegar a sufrir el espacio físico en el que se encuentra la empresa.

¿Para qué sirve?

Grupo de medidas enfocado a minimizar amenazas como:
- Desastres naturales
- Robos o sabotajes
- Actos de vandalismo

Medidas de seguridad física

1. Implementa **controles de acceso e interior**:
   - Control de acceso al recinto
   - Autenticación de usuario
   - Niveles de privilegio
   - Alarmas y CCTV
2. Instaura medidas de **restricción de accesos**:
   - Al CPD (Data Center)
   - A espacios de guarda de archivos físicos

5

SEGURIDAD LÓGICA

¿Qué es?

Aplicación de barreras, procedimientos y configuraciones adecuadas en los sistemas informáticos para proteger el acceso a sus datos e información.

¿Para qué sirve?

Proteger la información que se procesa, almacena y transmite para que sea siempre utilizada de forma autorizada y evitar acciones que puedan provocar su alteración, borrado o divulgación no autorizada.

¿Dónde se aplica?

- Puesto de trabajo(Endpoint)
- Disp. móviles y comunicaciones
- Red e infraestructura
- Aplicativos




Seguridad en el puesto de trabajo (Endpoint)

1. Implantar una **política de contraseñas** robusta tanto para el acceso al sistema operativo como a las aplicaciones.

2. Mantener **parches y actualizaciones** de seguridad, actualizando periódicamente servidor, programas y S.O.

3. Configurar los **roles de usuario** y los niveles de privilegio.

4. Implantar **soluciones de seguridad integral** para los terminales mediante antivirus y antimalware.

5. Restringir los **puertos USB** a puestos determinados y proporcionar a los usuarios herramientas de **cifrado**.

6. Controlar el **acceso remoto** hacia la organización mediante la instalación de sistemas del tipo VPN que garanticen su seguridad.

Seguridad en dispositivos móviles y comunicaciones

1. Creación de contenedores cifrados en los dispositivos que tengan datos confidenciales o accedan al correo de empresa.

2. Gestión de los dispositivos por parte de la empresa para controlar el uso y contenido empresarial del dispositivo.

3. Implementar sistemas de autenticación de múltiple factor.

4. Cifrado de las comunicaciones de datos mediante VPN's.

5. Cifrado de llamadas de voz en caso de tener comunicaciones confidenciales.

Seguridad en redes e infraestructura

1. **Cifrado de datos** confidenciales de la empresa, incluido el correo electrónico.

2. Implementar medidas **de seguridad** de la red: firewalls de nueva generación, routers y switches actualizados, etc.

3. Establecer un **aislamiento de redes**, por ejemplo, una red wifi para invitados.

4. Implantar medidas de **prevención de pérdida de datos** (DLP), orientadas también a la monitorización y control.

5. Introducir **sistemas de detección y prevención de intrusos** que frenen accesos no autorizados, como IPSs o sistemas NAC.

6. Realizar **copias de seguridad y pruebas de restauración** periódicamente.

Seguridad en los aplicativos

Aplicativos estándar o comercializados

1. Deben estar actualizados con parches y mejoras.

2. Establecer gestión y vigilancia de esas actualizaciones.

3. Trabajar en un entorno de preproducción de aquellas aplicaciones críticas para el negocio.

Aplicativos desarrollados o propios

1. Asegurarse de que pasan los estándares de seguridad.

2. Controlar quién accede a ellas y con qué privilegios.

3. Establecer un sistema de autenticación único para cada usuario (Single Sign-On).

6

SEGURIDAD DE LA INFORMACIÓN

¿Qué es?

Técnicas y medidas para controlar todos los datos que se manejan dentro de una institución y asegurar que no salgan de ese sistema.

¿Para qué sirve?

Asegura:
-La confidencialidad
-La disponibilidad
-La integridad
De los datos, haciendo frente a los riesgos, analizándolos y previéndolos.

Medidas para mantener la seguridad de la información de la empresa:

- Cifrado de la información, los soportes que la almacenan y las comunicaciones.
- Realizar copias de seguridad periódicamente.
- Utilizar contraseñas robustas.
- Realizar las actualizaciones de software correspondientes con los parches de seguridad de los sistemas.
- Controlar el acceso de los usuarios a la información. Principio del mínimo privilegio.

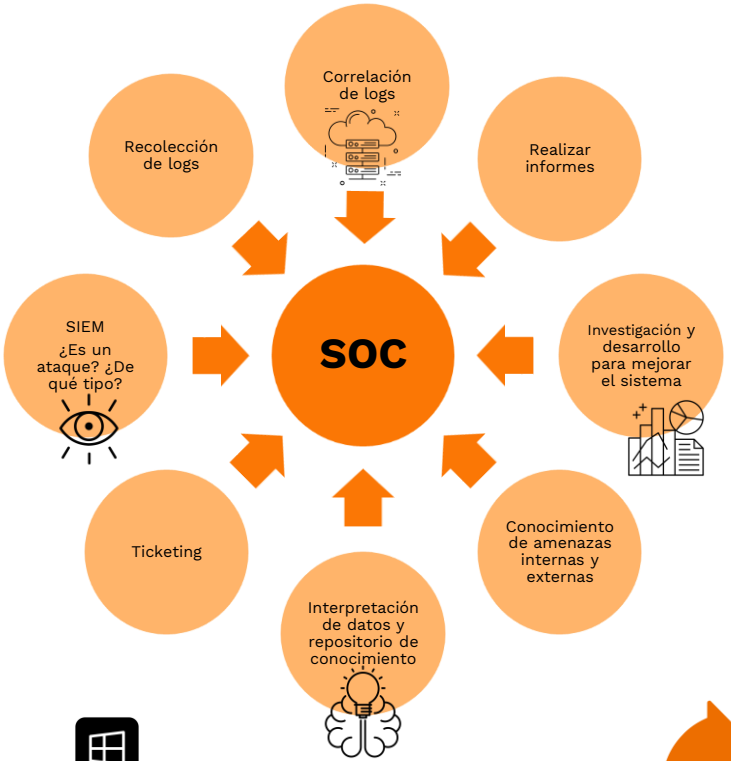
7

MONITORIZACIÓN

Una de las medidas para la monitorización del sistema de seguridad de una empresa es la **contratación de un SOC** (Security Operations Center)

El **SOC** se encarga de **monitorizar** y **actuar** (prevenir o resolver) atendiendo al contexto de seguridad.

Se trata de un **ciclo continuo** para conocer en todo momento el estado de seguridad de la empresa y actuar en consecuencia.



By mrHouston

DATA&TECH SOLUTIONS

¿Hablamos?

+34 91 432 02 86

info@mrhouston.net

www.mrhouston.net

¿Te ha gustado? Si quieres recibir más contenido como éste, puedes darte de alta aquí en nuestro blog de ciberseguridad y te enviaremos **(no más)** de un artículo al mes.
Además, tenemos más secciones que pueden interesarte.
¡Queremos conocerte!

En mrHouston nos dedicamos al desarrollo, implantación y mantenimiento de todo tipo de plataformas tecnológicas en el área de los sistemas de información.

Somos un equipo de personas que ofrece soluciones para **maximizar el valor** de las empresas.

No vendemos tecnología ni terminología incomprensible. Esa es nuestra diferencia. ¿Necesitas servicios de ciberseguridad? Contacta con nosotros. **Seguro que nos entendemos.**

AVISO LEGAL