**Aspectos a considerar para la página.**

Somos una consultoría especializada en brindar soluciones de seguridad informática a pequeñas empresas de México. Nuestro enfoque está en proteger tu negocio y garantizar la seguridad digital en la información.

**Servicios**

**Identificación y gestión de riesgos de seguridad**

Este proceso implica analizar vulnerabilidades, evaluar amenazas y medir el impacto potencial de los riesgos. Una gestión eficaz incluye desarrollar estrategias preventivas, aplicar controles correctivos y monitorear continuamente el entorno. ¡Mantenga su empresa segura!

**Implementación de medidas preventivas**

Establecer controles preventivos, así como llevar a cabo la monitorización. ¡Confíe en nosotros!

**Capacitación en seguridad informática**

Se imparte la enseñanza de prácticas como el manejo seguro de contraseñas, la identificación de correos maliciosos y la protección de datos sensibles. Además, se fomenta una cultura de prevención y responsabilidad entre los colaboradores.  ¡La seguridad es lo primero!

**Preguntas frecuentes**

1. **¿Qué tipo de información es la que debo proteger?**

La información que se debe proteger son los datos personales principalmente, un **dato personal** es cualquier información relacionada contigo, por ejemplo, tu nombre, teléfono, domicilio, fotografía o huellas dactilares, así como cualquier otro dato que pueda identificarte.

Es muy importante que cuides estos datos por razones de seguridad y porque es tu derecho; tus datos deben ser protegidos contra el mal uso como robo de identidad, transmisiones indebidas o accesos no autorizados.

1. ¿Cuál información se considera sensible?

La información sensible, también conocida como datos sensibles, se refiere a datos personales que requieren mayor protección debido a su carácter íntimo o el riesgo de discriminación o daño que su uso indebido podría generar. Incluye datos sobre origen racial, étnico, opiniones políticas, creencias religiosas, afiliación sindical, datos genéticos, biométricos, salud, orientación sexual, entre otros.

1. ¿Cómo puedo proteger mi empresa de amenazas cibernéticas?

Se deben implementar medidas de seguridad como la instalación de software de seguridad, la implementación de políticas de seguridad, la educación del personal y la vigilancia constante de la red. Se recomienda usar firewalls, antivirus, sistemas de detección de intrusiones y la autenticación multifactor.

1. ¿Qué medidas preventivas implementan en su servicio?

Se implementan cifrado de datos, políticas de seguridad en las cuales se deben realizar respaldos, monitoreo constante, cifrado de datos para minimizar los riesgos de que se pueda afectar la información.

1. ¿Ofrecen capacitación en seguridad informática personalizada?

Si, ofrecemos capacitación personalizada para el equipo de trabajo, enseñándoles buenas prácticas de seguridad informática y la manera de cómo reconocer posibles amenazas y poder prevenirlas.

<https://subeagenciadigital.com/lp/ciberseguridad-y-desarrollo/?utm_source=Google&utm_medium=Paid&utm_campaign=Ciberseguridad&gclid=Cj0KCQjw5azABhD1ARIsAA0WFUGBWGRzIYzIQX7ZLdyZA__xLjHLaAySwmwuE5v0efv8yJKPnB-Aqa4aAi3REALw_wcB&gad_source=1&gbraid=0AAAAADJtXMm0LvSvuIZbA9NIATbNc4tZn>

Podrás copiar este formulario que viene en esta página por favor.