Seguridad

Identificación
Prevención
Protección
Recuperación

Ciberseguridad ¡El delito es no estar preparado!

IDENTIFICACIÓN

CUMPLIMIENTO NORMATIVO Y LEGAL

- PCI-DSS
- ENS
- ISO27001
- RGPD

AUDITORÍA DE SEGURIDAD

- AUDITORÍA WEB HACKING
- TEST DE INTRUSIÓN
- AUDITORÍA DE BASTIONADO DE SISTEMAS
- DIAGNÓSTICO PYME
- AUDITORÍA DE CÓDIGO FUENTE
- **PAQUETIZACIÓN** HACKING PYME

PREVENCIÓN

GESTIÓN DE VULNERABILIDADES

- GESTIÓN ONLINE DE LA SEGURIDAD (SOC)

PROTECCIÓN

SOLUCIONES GESTIONADAS DE SEGURIDAD

- SEGURIDAD PERIMETRAL
- ENDPOINT PROTECTION
- MOVILIDAD EMPRESARIAL SEGURA
- INFRAESTRUCTURA WIFI SEGURA
- VIRTUALIZACIÓN DEL PUESTO DE TRABAJO
- BASTIONADO DE SISTEMAS

RECUPERACIÓN

SERVICIOS DE RECUPERACIÓN

- DISASTER RECOVERY SERVICE
- DISASTER RECOVERY SITE AS A SERVICE
- AUDITORÍA FORENSE

01 Consultoría: cumplimiento normativo y legal

Adecuación a estándares y buenas prácticas orientados al cumplimiento normativo exigido o recomendado según la actividad de cada Organización.

Servicio 'llave en mano' que incluye: **definición del alcance, análisis inicial, implementación de medidas correctivas y acompañamiento durante el proceso de certificación**.

RGPD

El nuevo Reglamento Europeo de Protección de Datos aporta una normativa única en toda la UE para aumentar la confianza y seguridad jurídica e impulsar la competencia justa. Introduce elementos como: el enfoque de riesgo, la figura del Responsable de Protección de Datos, privacidad desde el derecho, nuevos derechos, etc.

ISO27001

Establece las bases de un SGSI (Sistema de Gestión de la Seguridad de la Información) utilizando como marco de referencia las 12 áreas de actuación definidas en el Código de Buenas Prácticas en Gestión de la Seguridad de la Información identificadas en la norma ISO/IEC 27002.

ENS

El Esquema Nacional de Seguridad, en adelante ENS, es un marco de referencia de obligado cumplimiento en las AAPP para la creación de un proceso de gestión de la seguridad de la información acorde a buenas prácticas. El ENS toma como modelo de referencia la norma ISO27000, adaptándola a las particularidades y necesidades específicas de las AAPPs.

PCI-DSS

Estándar de seguridad que define el conjunto de requerimientos para gestionar la seguridad, definir políticas y procedimientos de seguridad, arquitectura de red, diseño de software y en medidas de protección que intervienen en el.tratamiento, procesado o almacenamiento de información de tarjetas de crédito.

02 Auditoría de seguridad

A través de técnicas basadas en Hacking Ético y buenas prácticas del sector, **bajo metodologías OWASP v4 | OSSTMM v3 | ISSAF Draft 0.2.1B | CIS Security**, nos encargamos de evaluar el estado de los sistemas de información frente a posibles amenazas, con el fin de identificar las vulnerabilidades que pudieran afectar tanto a su operativa normal, como revelar información sensible o provocar accesos no autorizados.

02.1 Auditoría Web Hacking

*Evaluaremos la **seguridad en los sistemas de comercio electrónico** (B2B/B2C) o **sistemas de gestión de contenidos** (CMS), **para identificar vulnerabilidades** que puedan ser explotadas por atacantes que intenten acceder o modificar información a la que no disponen de autorización.*

02.2 Test de Intrusión

*Evaluaremos la **seguridad de sus sistemas de información desde el exterior** de su organización (Correo electrónico, Acceso remoto, etc.), **igual que lo ejecutaría un atacante externo** identificando y explotando fallos de seguridad existentes.*

*Adicionalmente, evaluaremos también la **seguridad de sus sistemas desde el interior** de su organización, igual que lo ejecutaría un atacante que hubiese tenido éxito en un ataque externo o un usuario malintencionado de la propia organización.*

02.3 Paquetización: Test de intrusión Hacking PYME

	P1	P2	P3
1 IP pública y 2 Servicios*	✔		
2 IP's públicas y 4 Servicios*		✔	
B2B/B2C			✔
	Desde 1.500 €	Desde 2.250 €	Desde 3.000 €

** Servicio = Web, FTP, Correo, Acceso Remoto RDS o CITRIX, VPN, ... Para cualquier otro escenario se valorará a medida.*

02.4 Diagnóstico Pyme

Evaluaremos el estado de salud de la seguridad de la información de su empresa, ***identificando los riesgos relacionados con el acceso lógico, copias de seguridad, políticas de actualización, BCP, DRP, etc.****, que amenazan el funcionamiento de su organización y qué aspectos debe mejorar.*

02.5 Auditoría de Código Fuente

Analizaremos el código fuente de las aplicaciones desarrolladas por su organización, durante el proceso de vida del desarrollo, a fin de ***identificar posibles desviaciones de seguridad y corregirlas*** *durante el proceso de desarrollo.*

02.6 Auditoría de Bastionado de Sistemas

Analizaremos las configuraciones de seguridad establecidas (política de contraseñas, auditorías, protocolos inseguros habilitados, redirección de tráfico, DoS, etc.) en los sistemas operativos, bases de datos y electrónica de red de su organización, para ***identificar si están alineados con las buenas prácticas del sector y protegerlos de posibles ataques.***

03 Gestión de vulnerabilidades

Una de las mejores prácticas para mantener los sistemas y aplicaciones seguras es la **monitorización en búsqueda de brechas de seguridad, comportamientos anómalos, intentos de acceso, etc.,** utilizando para ellos herramientas de escaneo.

Gestión Online de la Seguridad (SOC)

Mediante nuestro ***SOC monitorizaremos y gestionaremos la seguridad en tiempo real de la infraestructura de su organización, aplicando "Inteligencia Artificial".*** *Esto nos permite la continua revisión de la seguridad sus sistemas, que es una práctica esencial para establecer una primera línea de defesa, pero esta actividad supone una carga de trabajo para los departamentos de IT, y requiere de un alto nivel de especialización.*

Por ello, INFORGES ofrece servicios completos de ***gestión de vulnerabilidades, tanto perimetrales como internos,*** *sustentados en herramientas de monitorización continua y servicios profesionales especializados en el descubrimiento de este tipo de vulnerabilidades, contribuyendo a mitigar el riesgo de padecer ataques a través del bastionado de sus sistemas de información.*

VENTAJAS

Disponer de sistemas y procesos seguros*, que afiancen la organización.*

Cumplir con la legalidad en materia de seguridad de activos*, evitando inspecciones y sanciones.*

Mejorar el uso de equipos e instalaciones*, haciéndolos más eficientes.*

Anticiparse y/o Reaccionar de forma temprana a incidentes de seguridad*.*

Priorizar las inversiones en equipos *para el tratamiento de información.*

Proteger la imagen corporativa e Incrementar la confianza de terceros*.*

04 Soluciones gestionadas de seguridad

La seguridad es un proceso continuo que requiere de una gestión altamente especializada. En Inforges ofrecemos **'Soluciones Gestionadas de Seguridad', bajo la modalidad de pago por uso mensual**, donde incluimos:

- **Los activos** (hardware y software) necesarios para la construcción del servicio.
- **Los servicios profesionales** para su puesta en marcha.
- **Los servicios de soporte, administración y evolución** del entorno.

Garantizamos la eficiencia del servicio ofrecido liberando al Departamento de IT de tiempos que puede dirigir a tareas más pegadas al negocio.

VENTAJAS

Innovación. Evolución continua del servicio y acceso y uso de últimas versiones 'de serie'.

No estocar. Paga solo por lo que usas.

Reducción de costes al consolidar servicios en un proveedor especializado.

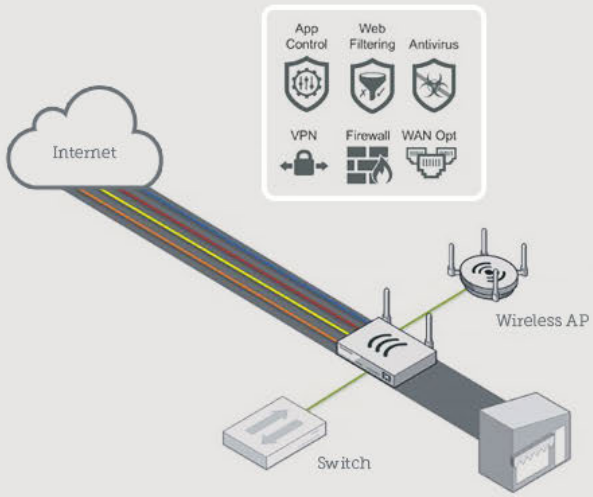
Liberar tiempos al equipo de TI del cliente para que éstos evolucionen de gestores de incidencias o gestores de proyectos.

Gasto de IT estable y predecible.

04.1 Seguridad perimetral

Analizamos la singularidad de cada cliente y seleccionamos la **Plataforma UTM** adecuada para ubicarla en sus instalaciones, realizando, entre otras, las siguientes funciones:

- **Protección de Red:** IPS, RED, VPN, HTML5, ATP, Security HearBeat.
- **Protección web:** antimalware, protección, visibilidad y filtro de aplicaciones y contenido.
- **Protección de correo electrónico:** Anti-Spam, SPX Mail Encryption y DLP.
- **Protección de Servidores Web:** Firewall de Aplicaciones y Proxi Inverso.
- **Sandbox Technology:** Junto con Intercept-X, proporciona la máxima defensa contra las últimas amenazas avanzadas como el ransomware.



Innovación constante mediante la actualización permanente de las últimas versiones de firmware y software, **gestión y administración del entorno** según las necesidades del servicio y **gestión de incidencias de seguridad** (intrusión, Infección,..) hasta su resolución.

04.2 Endpoint Protection

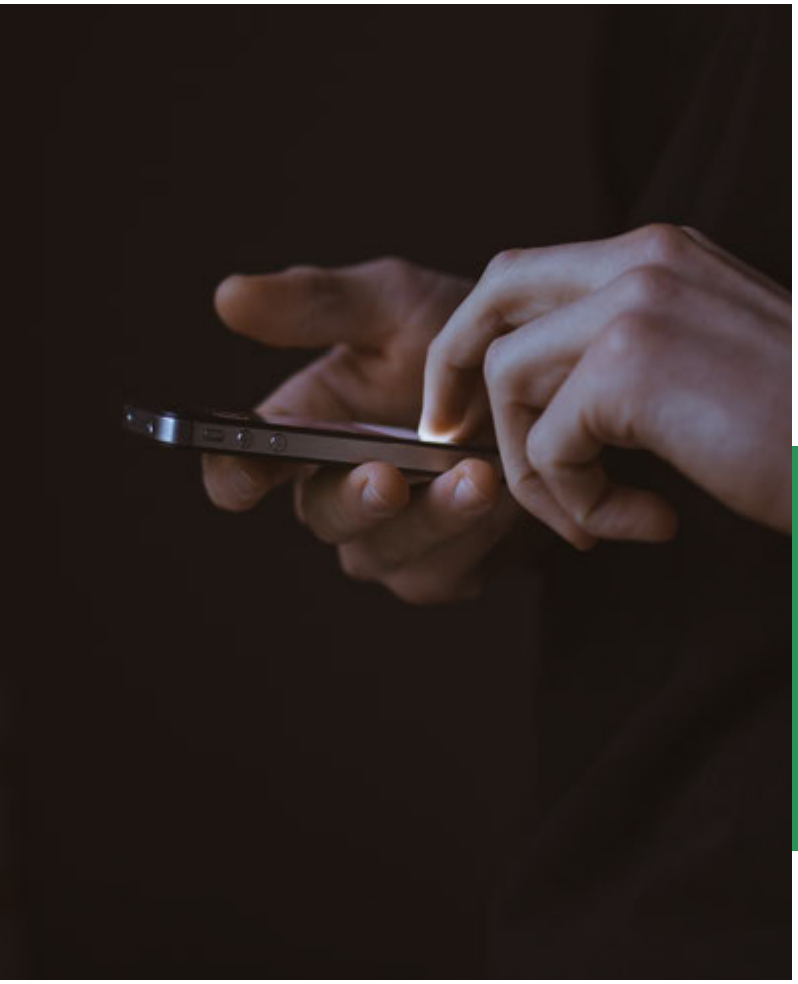
Solución integral de seguridad para usuarios y datos que incluye los siguientes servicios:

- **Motor avanzado de antivirus y antimalware**.
- **Prevención de fuga de datos DLP**.
- **Seguiridad Sincronizada e integrada con la seguridad perimetral** (siempre que se contraten ambos servicios), permite elevar el nivel de seguridad al 'correlacionar' el análisis del firewall y antivirus.
- **Encriptación del dispositivo** (opcional).
- **Antiransomware Intercept X** impide el cifrado malicioso y espontáneo de datos por parte de Rasomware. Incluso archivos o procesos de confianza que hayan sido secuestrados. Y una vez que se ha interceptado el ransomware, CryptoGuard revierte sus archivos a su estado seguro (opcional).

04.3 WIFI Segura

Estudio de cobertura y despliegue de infraestructura WIFI en oficinas, almacenes y entornos industriales, para dar cobertura en movilidad de forma segura. Analizaremos la singularidad de cada cliente y seleccionaremos el modelo y distribución de AP y el tipo de controlador más adecuado para ubicarlos en sus instalaciones.

- **Consola Gráfica accesible por el cliente** para análisis detallado de lo que ocurre en su Red: APs, Usuarios, Sesiones, etc...
- **Zona de Accesos para invitados**
- **Detección y eliminación de puntos de accesos no autorizados**
- **Seguridad Sincronizada con Mobile y Endpoint** en breve.



04.4 Movilidad segura

Solución de gestión de movilidad empresarial (EMM) para las empresas que desean dedicar menos tiempo y esfuerzo a la administración y a la protección de los dispositivos móviles. **Mantenga a los usuarios productivos, los datos empresariales seguros y los datos personales privados.** Incluye:

- **Gestión de dispositivos móviles.**
- **Gestión de aplicaciones móviles.**
- **Gestión del contenido móvil.**
- **Mobile Security y mucho más.**

Productividad: Deje que los usuarios trabajen donde quieran y en los dispositivos que quieran, de forma segura.

Seguridad: Asegúrese de que los datos empresariales no se pierdan nunca y de que no sean presa del malware.

Simplicidad: Fácil de configurar, administrar y mantener.

Valor: Con precios basados en usuarios, puede proteger los dispositivos de forma asequible.

04.5 Virtualización del puesto de trabajo

El modelo tradicional de aprovisionamiento, gestión y administración de Puestos de Trabajo no es sostenible, es cada vez más ineficiente y menos seguro.

Y es que **el Endpoint, hablando en el tándem que forma el usuario con el dispositivo, PC o portátil, siempre es el eslabón más débil.**

La virtualización de escritorios y puestos de trabajo traslada la ejecución descontrolada de aplicaciones y datos en dispositivos finales a un entorno seguro y custodiado en el CPD. **Todo duplicado, encriptado, aplicaciones y datos controlados. Con mecanismos de continuidad de negocio 'de serie': Todo actualizado, funcionando y alta disponibilidad con plan de Disaster Recovery.**

El puesto de trabajo como un servicio y de pago por uso mensual.

04.6 Bastionado de Sistemas

Adaptaremos las configuraciones de seguridad establecidas en los sistemas (sistemas operativos, bases de datos, electrónica de red) de su organización a las **buenas prácticas del sector y/o fabricante, para protegerlos de ataques de ciberseguridad:**

- Políticas de **contraseñas y Configuraciones de Auditorías.**
- **Permisos y Niveles de administración asignados.**
- Prevención de **acceso a usuarios anónimos.**
- Prevención de **denegación de servicio.**
- **Redirección de tráfico de red** a routers maliciosos.
- Deshabilitar **protocolos de red** y componentes innecesarios.
- Nivel de **parches de seguridad** y versionado.

05 Servicios de recuperación

En contra de la opinión generalizada, las situaciones de contingencia no son sólo provocadas por grandes desastres poco habituales y lejanos a nosotros. Muchos otros se producen con mayor frecuencia y con gran impacto en tiempo, recursos y negocio.

Nuestras soluciones permiten mantener la protección de datos y cargas de trabajo TI críticos para el negocio alineando el plan de continuidad de sistemas con la estrategia de negocio.

- **Réplica en infraestructura cloud en alta disponibilidad de los datos críticos.**
- **Requerimientos basado en criterios de tiempo de recuperación (RTO) y retención (RPO) objetivo**
- **Protección de inversión TI existente.**
- **Soluciones flexibles y escalables para adaptarse a nuevos riesgos.**

05.1 Disaster Recovery Service

Permiten disponer de una **copia de seguridad asíncrona** *en la Nube de los servidores virtuales disponibles en plataforma local (**DRS**).*

Diseñado y gestionado por Inforges para garantizar la disponibilidad de las copias de seguridad y asegurar la correcta recuperación en caso de fallo.

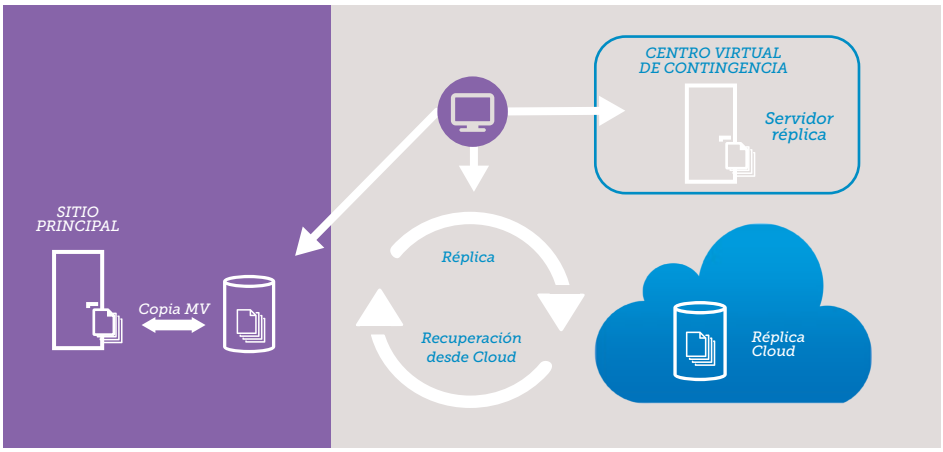
Doble copia de los datos: Local y remoto.

Pago por uso. Sólo por las MVs respaldadas en nuestro centro de datos.

Seguro. ***Cifrado de datos de extremo a extremo.***

05.2 Disaster Recovery SITE as a Service

Y, en caso de desastre o fallo, la posibilidad de activar el ***Centro de Respaldo Virtual*** *en cualquier momento para recuperar los servidores virtuales protegidos en un entorno Cloud (**DRaaS**).*



05.3 Auditoría Forense

La información sensible (contratos, acuerdos, precios, márgenes, etc.) es uno de los principales activos de su organización, por ello, supone un alto impacto cuando se tiene sospechas de lealtad de un empleado o exempleado.

INFORGES ofrece la ***asistencia técnica de expertos en Auditoría Forense, para la obtención y el posterior análisis de dispositivos, en investigaciones de fuga de información y eliminación de datos****, con objeto de confirmar las sospechas e intentar identificar la información sustraída. En caso de eliminación o daño de la información, disponemos de un* ***servicio de recuperación de información eliminada o dañada****, siempre y cuando sea posible.*

Inforges Murcia

C/ Vicente Aleixandre, 13
30011 Murcia
Tel.: 968 350 011
Fax: 968 264 569

Bilnea Murcia

Carril Condomina, nº 3, 10ºC
(Atalayas Business Center)
30006, Murcia.
Tel.1: 968 168 456
Tel.2: 633 170 511

Inforges/Bilnea Valencia

Gran Via del Marqués del Turia, 49.
Oficina 801
46005 Valencia
Tel: 961 155 808