

# DOSSIER CORPORATIVO



Ingeniería y Seguridad Informática



Avd. Central Nº 36, 1º Izda  
31010 Barañáin (Navarra)  
Teléfono-Fax: 948 10 19 22  
E-mail: [info@segurdrone.com](mailto:info@segurdrone.com)  
[www.segurdrone.com](http://www.segurdrone.com)

## ÍNDICE DE CONTENIDOS.

---

---

<b>1.- SEGURIDAD INFORMÁTICA</b> .....	3
1.1.- <i>CONCEPTOS BÁSICOS</i> .....	3
<b>2.- SERVICIOS OFRECIDOS RELACIONADOS CON LA SEGURIDAD INFORMÁTICA</b> .....	3
2.1.- <i>AUDITORÍAS DE SEGURIDAD</i> .....	3
2.2.- <i>SEGURIDAD PERIMETRAL</i> .....	4
2.3.- <i>CONTROL DE APLICACIONES</i> .....	5
2.4.- <i>CIFRADO DE SISTEMAS</i> .....	5
2.5.- <i>SISTEMAS DE BACKUP</i> .....	6
2.6.- <i>ELABORACIÓN DE UN PLAN DE CONTINGENCIA</i> .....	6
2.7.- <i>INFORMÁTICA FORENSE</i> .....	7
2.8.- <i>NORMATIVA Y LEGISLACIÓN</i> .....	7
<b>3.- APLICACIONES DE SEGURIDAD PERSONALIZADAS</b> .....	7
3.1.- <i>INGENIERÍA SOFTWARE</i> .....	8
<b>4.- SEGURIDAD EN ENTORNOS DOMÓTICOS</b> .....	8
4.1.- <i>SISTEMAS DE VIDEOVIGILANCIA</i> .....	8
4.2.- <i>SISTEMAS DE ALARMAS</i> .....	9
4.3.- <i>SENSORIZACIÓN Y CONTROL REMOTO</i> .....	9
<b>5.- INVESTIGACIÓN, DESARROLLO E INNOVACIÓN (I+D+I)</b> .....	9

## 1.- SEGURIDAD INFORMÁTICA

Actualmente tanto empresas como particulares han convertido el uso de la Informática y de Internet en algo cotidiano e imprescindible. Pero a pesar de ello la seguridad de la información continúa siendo algo opcional para la mayoría de ellos.

La seguridad informática, sigue siendo una de las asignaturas pendientes de muchas empresas. Cada día la seguridad es violada por hackers y usuarios que acceden a información sensible o privilegiada, haciendo uso de ella o realizando operaciones no permitidas.

La seguridad consiste en certificar que los recursos del sistema de información de una organización son utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas para ello. Resumiendo, la Seguridad Informática está vinculada con la protección de los sistemas informáticos y de la información.

### 1.1.- CONCEPTOS BÁSICOS

Cuando hablamos de entorno o sistema seguro, es un término demasiado amplio y complejo por lo que hablaremos de fiabilidad, de tal forma que definamos un sistema seguro como aquel que se comporta como se espera de él. Todo Sistema fiable ha de cumplir cinco requisitos.

- **Disponibilidad:** La información y recursos han de estar siempre disponibles para el personal autorizado.
- **Integridad:** Toda información almacenada o en circulación por la red, debe de estar protegida contra la modificación no autorizada.
- **Autenticidad:** No solo hemos de estar seguros de que el contenido es el correcto, además hemos de garantizar que alguien es quien dice ser.
- **Confidencialidad:** Difusión no autorizada de la información, nuevamente, solo aquel que esté autorizado podrá acceder a determinados recursos.
- **No repudio:** Mecanismo necesario que impide que alguien pueda negar que haya realizado una determinada comunicación (enviar un mensaje por ejemplo)

## 2.- SERVICIOS OFRECIDOS RELACIONADOS CON LA SEGURIDAD INFORMÁTICA:

### 2.1.- AUDITORÍAS DE SEGURIDAD:

Toda empresa con un tamaño mínimo ha de tener una auditoría informática independiente, que garantice la seguridad de sus sistemas, bases de datos, fuga de activos... capaz de prever y detener tanto ataques internos como externos.

Mediante una auditoría informática se realiza una evaluación de los sistemas cuyo fin es detectar errores y fallos, entregando un informe detallado con las deficiencias detectadas y el plan de acción necesario para mitigar los riesgos.

### *¿Qué servicios ofrecemos?*

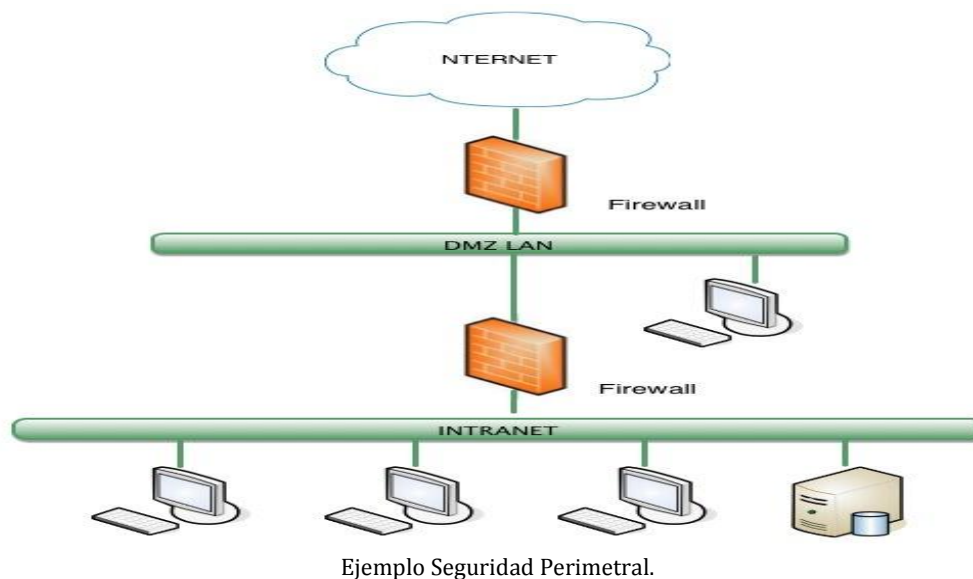
- Auditoría de seguridad interna.
- Auditoría de seguridad externa.
- Test de intrusión.
- Auditoría Hacking Ético: Se trata de analizar y evaluar la situación actual de las arquitecturas frente a ataques tanto internos como externos, adoptando el perfil de un atacante malintencionado.
- Auditoría WLAN de seguridad WIFI: En la redes WLAN el medio es compartido por lo que en definición ya son inseguras. Si además sumamos que algunos de los sistemas de seguridad más utilizados son fácilmente quebrantables (WEP), hace que nos planteemos seriamente la seguridad de la arquitectura de la red inalámbrica. Por todo esto, proponemos una auditoria específica para la seguridad de las WLAN.
- Reparación definitiva de todos los problemas encontrados.

## **2.2.- SEGURIDAD PERIMETRAL:**

La Seguridad Perimetral es uno de los posibles métodos de defensa de una red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto nos permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios y denegando cualquier tipo de acceso a otros.

### *¿Qué servicios ofrecemos?*

- Gestión de tráfico de red.
- Firewall y Routing: El Firewall es una parte de un sistema informático diseñado para bloquear el acceso no autorizado. Se trata de un dispositivo configurado para permitir o denegar las transmisiones de red basada en un conjunto de normas y otros criterios.
- Protección contra malware.
- Filtrado de contenido.
- VPN Seguras.
- Integración IDS y HIDS: Los sistemas de detección, basados en usos incorrectos, simplemente monitorizan las actividades que ocurren en un sistema y las comparan con una serie de firmas de ataques previamente almacenados en una base de datos, cuando se monitoriza una actividad que coincide con una firma se genera una alarma.



### 2.3.- CONTROL DE APLICACIONES:

Las aplicaciones son uno de los elementos clave en los ambientes de tecnologías de la información, pero también son uno de los más ignorados con lo que respecta a la seguridad. Actualmente se considera oportuno gestionar el control de acceso a las diferentes aplicaciones y se presupone como suficiente, pero no es así, la seguridad en estas aplicaciones debería ser una seguridad nativa y por lo tanto más robusta.

Un factor clave en la seguridad de las aplicaciones es la gestión de identidades, validando así los usuarios que acceden al sistema, permitiendo el uso de perfiles o roles de usuario, dotando a cada uno de ellos de los recursos necesarios para el desempeño de su tarea y limitando el acceso a aquellos recursos y datos que no son de su incumbencia.

Un claro ejemplo de uso del control de aplicaciones se da en entornos industriales. Si no somos capaces de limitar el acceso a determinados servicios, un intruso malintencionado es capaz de paralizarnos toda una cadena de producción.

#### *¿Qué servicios ofrecemos?*

- Autenticación robusta.
- Gestión de identidades.
- Single sign on (ESSO).

### 2.4.- CIFRADO DE SISTEMAS:

La criptografía es sin duda la mejor técnica para mantener la información lejos del alcance de un atacante, incluso en el caso de que un intruso consiga burlar todos los elementos de seguridad de una red, si se utiliza un buen sistema de cifrado, este no podrá obtener la información confidencial de la organización.

En una comunicación cliente-servidor nos permite garantizar que el emisor es quien dice ser, y además garantizar que el contenido del mensaje no ha sido alterado. De esta forma evitamos espionaje de correos electrónicos.

#### *¿Qué servicios ofrecemos?*

- Criptosistemas simétricos, basados en clave secreta.
- Criptosistemas asimétricos, basados en clave pública.
- Firma digital: Una vez cifrado un documento lo firmamos digitalmente, asegurándonos autenticidad, integridad y no repudio.
- Protocolos criptográficos como SSH: SSH permite acceder a máquinas remotas a través de una red, permitiendo manejar por completo un equipo mediante el intérprete de comandos.
- Certificados digitales SSL/TLS: Seguridad en capa de transporte, mediante certificados digitales conseguimos verificar que el servidor es quien dice ser.

#### **2.5.- SISTEMAS DE BACKUP:**

Este servicio permite almacenar una copia de los datos informáticos de su empresa de forma externa automatizada y segura, garantizando así la máxima seguridad de estos y su completa disponibilidad, ya que usted podrá acceder y restaurar sus datos siempre que lo desee.

Mediante este servicio su empresa no necesita recursos propios para realizar las copias de seguridad, el copiado es automático y personalizable.

#### *¿Qué servicios ofrecemos?*

- Consultoría Backup.
- Backup remoto y continuo.
- Recuperación de sistemas.
- Servicio Disaster Recovery.

#### **2.6.- ELABORACIÓN DE UN PLAN DE CONTINGENCIA:**

Es una herramienta que nos ayudará durante los procesos críticos de una empresa u organización, para que esta continúe funcionando a pesar del posible fallo en los sistemas informáticos. Se podría definir como una estrategia planificada, estableciendo una serie de procedimientos que nos guiarán para restituir rápidamente los servicios de la organización ante una eventualidad que pueda paralizar de forma total o parcial el funcionamiento habitual de nuestro sistema de información.

#### *¿Qué servicios ofrecemos?*

- Elaboración de un Plan de Contingencia.
- Sensibilización de los empleados.

## 2.7.- INFORMÁTICA FORENSE:

Robos de información, fraude, manipulación o abusos de los correos electrónicos, ataques a web, acceso no autorizado... son algunos de los posibles ataques que puede sufrir nuestra organización, todos ellos dejan tras de sí un rastro difícil de seguir. Con la informática forense se pretende investigar, obtener y evaluar las pruebas encontradas en los diferentes sistemas.

### ¿Qué servicios ofrecemos?

- Adquisición de evidencias.
- Análisis forense de dispositivos móviles.
- Análisis forense de sistemas y equipos.

## 2.8.- NORMATIVA Y LEGISLACIÓN

### ¿Cuál es la normativa y legislación tecnológica?

En España los sistemas informáticos que trabajan con datos personales se encuentran regidos actualmente por tres leyes.

- Ley Orgánica de Protección de Datos, LOPD.
- Ley General de Telecomunicaciones.
- Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.

La LOPD indica que se deben adoptar las medidas técnicas necesarias para garantizar la seguridad de los datos personales, evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Las herramientas de control de contenidos previenen la difusión, accidental o intencionada, de cualquier tipo de información o datos fuera de una organización. Evitan la fuga de información a través de correo electrónico, mensajería instantánea, transferencia de fichero mediante FTP, red P2P, chat, blog, o mediante dispositivos externos de almacenamiento como es el caso de memorias USB. Actúa monitorizando todo tipo de canal de comunicación, desde y hacia el exterior de la organización implementando políticas de uso de información sensible.

### ¿Qué servicios ofrecemos?

- Asesoramiento e implantación de políticas de uso de información.

## 3.- APLICACIONES DE SEGURIDAD PERSONALIZADAS.

Con la intención de fomentar la seguridad de forma global, convirtiéndose en un factor transversal que cubra todos los ámbitos de una organización, ofrecemos

unos planes de seguridad personalizados, entre los que incluimos diferentes servicios como por ejemplo:

### 3.1.- INGENIERÍA SOFTWARE

Empresas y organizaciones pueden encontrar un atractivo conjunto de soluciones de software, que aumenten su producción o disminuyan el coste de las mismas. Todo esto mediante el desarrollo de aplicaciones personalizadas, ajustadas a sus requerimientos, eso sí, siempre con el objetivo de aumentar la seguridad de su organización tanto digital como física.

#### ¿Qué servicios ofrecemos?

- Programación de autómatas y PLC, dispositivos empleados en automatización industrial, mejorando el proceso de fabricación y creando un entorno más seguro para el empleado.
  - Gestión de alarmas.
  - Gestión de retardos en los temporizadores.
- Aplicaciones para Smartphone: Aprovechando la tecnología de los dispositivos móviles y la gran repercusión que están teniendo este tipo de dispositivos en el mercado actual, ofrecemos la posibilidad de desarrollar aplicaciones capaces de comunicarse con otros dispositivos y que nos ayuden a mejorar la producción y la seguridad, siendo esta accesible desde cualquier lugar.
  - Posicionamiento GPS.
  - Acelerómetro y giroscopio.
  - Efectos de cámara a tiempo real.

## 4.- SEGURIDAD EN ENTORNOS DOMÓTICOS.

---

Ofrecemos la posibilidad de desarrollar, implementar y mantener soluciones de software a medida para nuestros clientes adaptándolos a sus necesidades y definiendo así un proyecto que cubra todos sus requerimientos, desde la propia infraestructura de las comunicaciones, los sistemas y las aplicaciones.

Estos servicios son ajustables desde hogares y supermercados, hasta grandes complejos hoteleros, por lo que cubre cualquier tipo de necesidad y entorno.

### 4.1.- SISTEMAS DE VIDEOVIGILANCIA.

- Videovigilancia en circuito cerrado.
- Videovigilancia inteligente: ofreciendo un servicio más eficiente y útil capaz de monitorizar y recibir, en tiempo real, avisos de los elementos significativos que están ocurriendo y cambiando así su funcionamiento.
- Videovigilancia por Internet.



#### **4.2.- SISTEMA DE ALARMAS.**

Sistema de alarmas desplegado en todo el recinto, ya sea mediante sensores, detección de intrusos... de forma que en el momento en que una de ellas es activada, es decir, salta, avisamos inmediatamente al responsable, ya sea policía, gerente, propietario...

#### **4.3.- SENSORIZACIÓN Y CONTROL REMOTO.**

Otro de los servicios que ofrecemos va más orientado al confort y reducción de consumo energético. Esto se consigue con un despliegue de sensores, ya sean lumínicos, de humedad o de temperatura, que interactúan con diferentes actuadores consiguiendo, por ejemplo, bajar la temperatura de una sala.

Además podemos disponer de un sistema de control remoto, ya sea centralizado en un mando a distancia o desde su propio terminal móvil, con el cual podremos actuar con todos los sensores y actuadores dispuestos en nuestro hogar o nuestra empresa.

### **5.- INVESTIGACIÓN, DESARROLLO E INNOVACIÓN (I+D+I)**

---

Los programas de Investigación Desarrollo e Innovación, también forman parte de nuestros servicios. Actualmente, estamos trabajando en el desarrollo de una aplicación de videovigilancia utilizando un vehículo aéreo no tripulado llamado Drone.

Esta aplicación supondría una revolución en algunos sistemas de vigilancia, además podría ser utilizada en otros ámbitos como por ejemplo exploración de zonas muy extensas como urbanizaciones, grandes fábricas, extensiones forestales, control de masas...

A grandes rasgos el sistema consta de un Drone, una cámara de alta definición y un receptor de la información. Establecemos un recorrido por el que se desplaza nuestro vehículo, en tiempo real nos envía la información al receptor y lo podremos visualizar en una pantalla, almacenar en un disco interno, modificar el recorrido de nuestro vehículo... en resumen, nos ofrece la posibilidad de inspeccionar zonas de forma remota y sin asistencia humana con la consiguiente minimización de riesgo físico. Estas inspecciones pueden darse tanto en entornos abiertos como en interiores.