CIBER101

¿Qué es CIBER101?

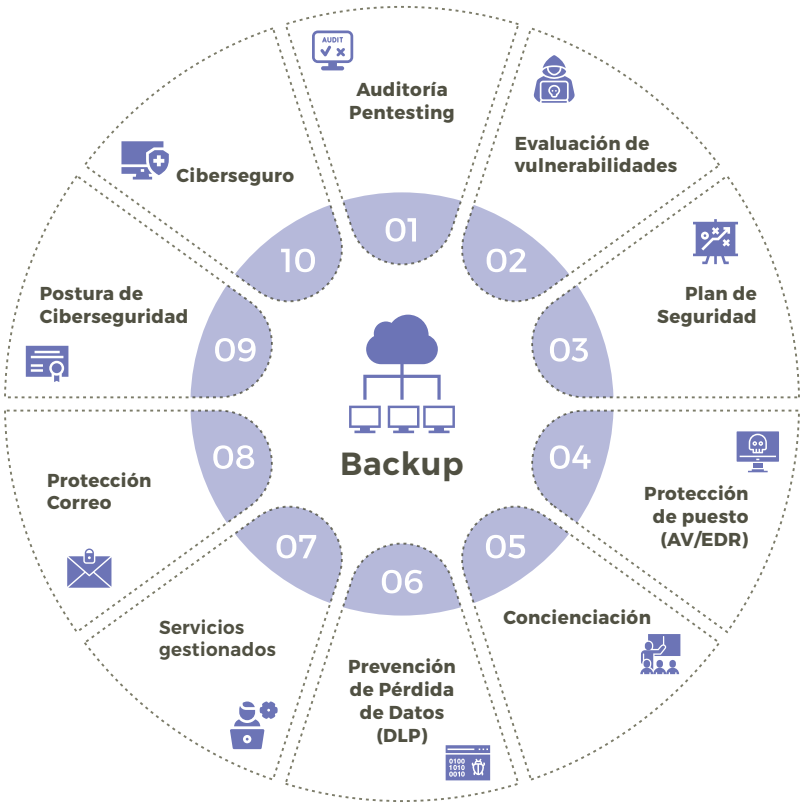
CONTÁCTANOS

Avda. Manoteras, 24. Planta 2
28050 Madrid
T. 910 600 101
M. info@datos101.com
W. www.datos101.com

Los servicios proporcionados dentro del paquete CIBER101 ayudarán a monitorizar, proteger y restaurar los datos de la organización en caso de sufrir un incidente de seguridad.

CIBER101 es un conjunto de servicios de ciberseguridad que permiten a cualquier compañía robustecer su postura de ciberseguridad con soluciones y servicios dimensionados al tamaño de la organización.

Desde Datos101 con nuestros servicios CIBER101 afianzamos la estrategia de protección de los datos, por esta razón contemplamos como primera medida el backup de datos sobre la que se construye el resto de la propuesta de soluciones y servicios ciber, además de estar cubierto por un ciberseguro que protegerá a la compañía en caso de un incidente de seguridad.



DATOS 101

¿Si no sabemos como estamos cómo vamos a protegernos?

Lo primero que debemos hacer antes de adoptar cualquier herramienta de ciberseguridad es saber cómo estamos y cuáles son los riesgos de ciberseguridad a los que se enfrenta o puede afrontar nuestra organización. Para ello debemos realizar un diagnóstico de la situación, además, realizar una auditoría o pentesting ligero para testear nuestra infraestructura tecnológica para averiguar cómo las amenazas pueden afectarnos y analizar las vulnerabilidades de dicha infraestructura.

Consideramos imprescindible incorporar desde la propuesta Plus, la adopción del EDR (Endpoint, Detection and Response) para proteger los puestos de trabajo y los servidores.

El primer firewall de las compañías es el usuario. Tanto nosotros como nuestros trabajadores debemos conocer las amenazas a las que tenemos que hacer frente en el uso diario de las herramientas tecnológicas de las que disponemos en nuestro día a día.

CIBER101 consta de tres paquetes en función de los servicios que se contraten y el número de puestos de trabajo de la compañía.

Se comercializa en tres formatos (Estándar, Plus y Premium) en función del nivel de servicio deseado. Además, disponemos de manera remota en función del paquete elegido de una capa de servicios gestionados con monitorización, soporte y mantenimiento. (¿De qué sirve la seguridad sin monitorización?)

Dentro de la evolución y la mejora de la postura de ciberseguridad de la compañía, se deberían incorporar soluciones más específicas para resolver amenazas concretas y, aquí, proponemos proteger el correo electrónico y la fuga de datos, el mayor activo de las empresas.

Finalmente para completar y limitar al máximo nuestro riesgo, consideramos necesaria la contratación de un ciberseguro.

Servicios	Estándar	Plus	Premium
Backup en nube por desktop (50GB) o de O365	☺	☺	☺
Análisis vulnerabilidades	☺	☺	☺
Evaluación vulnerabilidades	☺	☺	☺
Protección puesto de trabajo: Antivirus	☺	☺	☺
Protección puesto de trabajo: EDR		☺	☺
Servicios gestionados EDR		☺	☺
Plan de seguridad		☺	☺
Concienciación (Formación usuarios)		☺	☺
Protección correo			☺
Prevención pérdida de datos (DLP)			☺
Certificado (Postura de Ciberseguridad)	☺	☺	☺
PVP Precio por mes	**8,50 €**	**15,00 €**	**22,00 €**

Componentes

Backup

Aseguramos los datos de las empresas con nuestras soluciones de copias de seguridad en la nube y recuperación de datos.

Con la copia de seguridad en la nube realizamos un backup de los archivos, aplicaciones, máquinas virtuales o servidores y se almacenan de forma segura en una red de recursos informáticos a los que se accede a través de Internet.

Acceso

Las organizaciones acceden a sus archivos en cualquier momento y en cualquier lugar donde tengan una conexión a Internet.

Protección

Los datos se encuentran aislados frente a fallos de dispositivos locales, ataques de malware o desastres naturales.

Inactividad

El sistema se restaura rápidamente para que las empresas puedan continuar su actividad.

Las principales características del servicio son:

- Disponibilidad 24x7: garantizamos el acceso a sus copias de seguridad a cualquier hora de cualquier día del año, los datos estarán disponibles cuando la empresa los necesite.
- Retención y versiones: La continuidad de la empresa está garantizada con nuestra política de retención de 180 días. Recuperarán los archivos de forma sencilla y trabajarán con normalidad en cuestión de segundos.
- Siempre informado: reciben los informes de estado de las copias de seguridad de la empresa en el intervalo de tiempo que deseen.
- Automatizado: una vez configurada la aplicación el software se ejecuta en segundo plano y no interferirá para nada en el trabajo.
- Sistema incremental: se ahorra tiempo y ancho de banda subiendo solamente las modificaciones y no todos los archivos.
- Máxima seguridad: Sistema de encriptación de 256-bits. Todos los archivos de la empresa son encriptados antes de salir del ordenador.
- Portal web: podrán consultar el estado e información de las copias de seguridad de la empresa siempre que lo necesiten.

Auditoría de ciberseguridad

Pentesting de la web y los servicios públicos de la empresa para comprobar las brechas de seguridad reales de la compañía. Ataques de esos entornos con el objetivo de detectar y prevenir posibles fallos (debilidades o vulnerabilidades).

Emulando las condiciones reales de un ataque por parte de un atacante que no posee información previa de la empresa, partiendo solamente de las direcciones IP públicas que se definan dentro del alcance, se realizarán las siguientes actuaciones:

- Descubrimiento de dispositivos, redes, servicios y protocolos mediante técnicas automáticas y posterior validación y revisión manual.
- Análisis de vulnerabilidades de servicios externos mediante técnicas automáticas y posterior verificación de las vulnerabilidades.

Evaluación de vulnerabilidades

Es importante mantener todos los sistemas esenciales para la empresa, desde estaciones de trabajo a servidores, actualizados con los últimos parches de software. Aunque se distribuyen con frecuencia nuevas correcciones para las vulnerabilidades, Con frecuencia se producen nuevas actualizaciones para corregir las vulnerabilidades, por lo que la administración puede ser difícil y lleva mucho tiempo.

El objetivo del servicio es la identificación de vulnerabilidades de los sistemas con el objetivo de asegurarse de que todas las aplicaciones y los sistemas operativos estén actualizados y no puedan ser atacados por los ciberdelincuentes.

Plan de ciberseguridad

De acuerdo con INCIBE, para garantizar la seguridad de la información del negocio se necesita llevar a cabo una gestión planificada de actuaciones en materia de Ciberseguridad, tal y como se realiza en cualquier otro proceso productivo de la organización.

El Plan consiste en la definición y priorización de un conjunto de medidas concretas a implantar en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles adecuados, a partir de un análisis de la situación inicial.

El Plan se alineará con los objetivos estratégicos de la empresa, incluirá una definición del alcance e incorporará las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la organización, así como terceros que colaboren con ésta:

- Iniciativas dirigidas a mejorar los métodos de trabajo actuales.
- Planteará un conjunto de acciones de mejora.

Endpoint Detection and Response (EDR)

EDR es un sistema proyectado para identificar, interrumpir y reaccionar frente a amenazas o ataques que se pongan en marcha a través de dispositivos terminales como ordenadores, tabletas, laptops y smartphones.

Implementado mediante la instalación de agentes de endpoints, puede gestionarse mediante un software en la infraestructura local o mediante un portal cloud.

En el nuevo paradigma tecnológico en el que se encuentran las empresas que presentan dinámicas remotas y necesitan proteger y monitorizar continuamente los endpoints distribuidos, las soluciones de EDR se muestran eficaces en la detección de malwares creados para evadir el descubrimiento de los sistemas antivirus tradicionales.

Algunas de las características de la solución de EDR propuesta:

- Detección avanzada: Utiliza técnicas avanzadas de detección, como análisis de comportamiento, análisis de firmas y aprendizaje automático, para identificar actividades sospechosas o maliciosas en los endpoints.
- Respuesta automatizada: Permite la respuesta automatizada a eventos de seguridad detectados, como el aislamiento de un endpoint comprometido o la terminación de procesos maliciosos.
- Análisis de amenazas en tiempo real: Monitoriza constantemente los endpoints en busca de indicadores de compromiso (IOCs) y señales de amenazas, y proporciona alertas y notificaciones en tiempo real para acciones rápidas.

Al implementar una solución EDR, las organizaciones pueden fortalecer su postura de seguridad al tener una visibilidad más profunda de los endpoints y la capacidad de detectar, investigar y responder rápidamente a las amenazas. Esto ayuda a reducir el tiempo de detección y respuesta, minimizando así el impacto de los ataques y mejorando la protección de los activos críticos de la organización.

Componentes

Concienciación

Nuestra plataforma Online de capacitación y concienciación en Seguridad de la Información permite generar comportamientos seguros en los usuarios, favoreciendo la creación de una cultura cibersegura.

Cursos y videos interactivos

La plataforma ayuda a los usuarios a retener información con videos cortos y aprendizaje interactivo. Mantiene a los usuarios informados con cursos cortos y sin jerga.

Utilizando los perfiles de riesgo de los empleados, se pude inscribir a los usuarios en programas de formación personalizados que aborden sus riesgos específicos, priorizando los temas de los cursos en función de sus áreas más débiles.

Comprender cómo los empleados están progresando, comparando el grado de riesgo de toda la empresa con en el desempeño de cada usuario.

Simulación de Phishing

Con personal nuevo, entornos de trabajo cambiantes y amenazas de phishing que evolucionan constantemente, la evaluación de riesgo continuo es crucial.

- Habilitar simulaciones regulares que vigilen el riesgo continuo del usuario.
- Ejecutar pruebas de phishing selectivo, haciéndose pasar por personal interno.
- Únicamente se realizarán sobre los correos corporativos.

Los modernos ataques de phishing suelen presentarse en forma de campañas dirigidas que se hacen pasar por personal interno. Con la elaboración de plantillas y la suplantación de dominios, testeamos a los usuarios con un "spear-phishing" dirigido.

Formación

Formación contextual a los usuarios inscribiendo automáticamente a los empleados en microcursos, cuando se vean comprometidos en una de las simulaciones.

Prevención de pérdida de datos (DLP)

Esta solución, descubre y protege los datos confidenciales, mientras supervisa las operaciones relacionadas con dicha información.

Los principales beneficios de su adopción son:

Amenazas internas

Impide las fugas de datos debidas a negligencias de los empleados o a personal interno malintencionado, bloqueando los intentos no autorizados de acceder o transferir datos, descubriendo y protegiendo los datos confidenciales en reposo.

Visibilidad de la protección de datos

Reduce la complejidad de la protección de datos y recorta el tiempo de generación de informes proporcionando una amplia visibilidad de los flujos de datos y del comportamiento de los usuarios.

Cumplimiento de normativas en los procesos

Reduce los riesgos para la seguridad de la información cumpliendo los estándares y normativas de seguridad de TI, mediante la aplicación de directivas de empleo y gestión de datos que los usuarios no pueden sortear.

Servicios gestionados

Se trata de un servicio gestionado cuyo principal objetivo es detectar y reaccionar adecuadamente ante amenazas que coloquen en riesgo los datos que la empresa maneja.

El servicio es un complemento recomendable e idóneo para gestionar y monitorizar la solución de EDR implementada, ofrecida por un equipo completo de seguridad.

Mediante un análisis avanzado de seguridad en endpoints, aplicaciones, comportamiento del usuario y redes.

A través del empleo de la Inteligencia Artificial y Machine Learning, somos capaces de aumentar la velocidad de detección y respuestas digitalizando los datos y automatizando las acciones.

Los principales servicios gestionados son los siguientes:

- **Detección de amenazas:** identificación actividades sospechosas o maliciosas en los sistemas de la organización en los que se encuentre implementado el agente de la solución EDR.
- **Monitorización continua:** monitorización constante de los endpoints de la organización donde se encuentre instalado el agente, para detectar y responder rápidamente a cualquier incidente de seguridad.
- **Informes y asesoramiento:** informes periódicos sobre la actividad de seguridad, las amenazas detectadas, y las recomendaciones para mejorar la postura de seguridad de la organización.

El servicio se complementa con la administración automatizada de parches que facilitan la protección de la empresa contra las últimas amenazas. Hasta que los parches no se instalan en todos los sistemas, la empresa sigue desprotegida frente a las ciberamenazas más avanzadas. Las evaluaciones de vulnerabilidades ayudan a las organizaciones a identificar sistemas y aplicaciones que requieren actualizaciones y a desplegar parches fácilmente, bajo demanda o de forma programada. Antes de aplicar nuevos parches con el fin de proteger los datos esenciales de la empresa y facilitar la reversión de los sistemas a un estado de funcionamiento anterior, en caso de necesidad, la creación automática de copias de seguridad del sistema completo.

Protección de correo

La adopción de este tipo de herramientas, mejora la seguridad de las empresas interceptando los ataques modernos del correo electrónico antes de que lleguen a los usuarios.

En consecuencia, las implantación de una herramienta de estas características bloquea las amenazas del correo electrónico –incluidos el spam, el phishing, los ataques BEC (vulneración del correo electrónico de empresas), la usurpación de cuentas, el malware, las amenazas persistentes avanzadas (APT) y los ataques de día cero– antes de que lleguen a la bandeja de entrada de Microsoft 365, Google Workspace o cualquier buzón o servidor de correo electrónico local o en la nube.

Los principales beneficios que pueden obtenerse se concretan en los siguientes puntos:

Detención del phishing y de los intentos de suplantación

Minimización del riesgo asociado al correo electrónico mediante inteligencia sobre amenazas completa, detección basada en firmas, comprobaciones de reputación de URL, algoritmos especiales de reconocimiento de imágenes, y aprendizaje automático con comprobaciones de registros DMARC, DKIM y SPF.

Identificación de técnicas de evasión avanzadas

Detección del contenido malicioso oculto gracias a que la solución descomprime de forma recursiva los archivos y URL adjuntos o incrustados, y los analiza por separado con motores de detección dinámica y estática, realizando un análisis profundo del 100 % del contenido.

Prevención de APT y ataques de día cero

Neutralización de las amenazas avanzadas que eluden las defensas convencionales con la exclusiva tecnología a nivel de CPU que bloquea los exploits antes de que se libere el malware y ofrece un veredicto en cuestión de segundos.

Componentes

Postura de seguridad

La realización de evaluaciones periódicas de la efectividad de las medidas adoptadas de seguridad, practicando pruebas de penetración y revisando regularmente las políticas y procedimientos, es crucial ante el desafío en constante evolución al que se enfrentan las organizaciones en su día a día.

Las regulaciones que nos vienen de Europa y que afectan a la ciberseguridad, abordan la seguridad de las cadenas de suministro y las relaciones con los proveedores, permitiendo a las empresas exigir a sus proveedores el cumplimiento de la normativa en caso de ser entidades designadas como operadores críticos. Esta medida obliga a tener una visión más global y completa de los riesgos en ciberseguridad de una organización.

Reiterando que la ciberseguridad es un proceso evolutivo, las organizaciones deben adoptar el modelo de mejora continua en su postura de seguridad. Por aplicación de las nuevas regulaciones, prácticamente la totalidad de las organizaciones se van a ver sometidas a controles periódicos por parte de sus clientes.

Con el objetivo de conocer el nivel de seguridad de la empresa y tomar este nivel de seguridad como punto de partida para diseñar e implantar las futuras mejoras de seguridad, dentro de la propuesta contemplamos la emisión de un certificado que demostrará al resto de nuestro ecosistema de negocio nuestro nivel de seguridad:

- Rating de ciberseguridad
- Detalle de la auditoria y análisis de vulnerabilidades
- Detalle de soluciones adoptadas
- Seguimiento del plan de seguridad
- Evaluación de concienciación
- Contratación de un ciberseguro

Ciberseguro

Según dicen los analistas, el ciberseguro es la póliza de incendios del siglo XXI.
La cobertura del ciberseguro comprende lo siguientes extremos:

- Suplantación de Identidad (transferencias fraudulentas)
- Respuesta Técnica a un ciberataque (atención especializada 24x7)
- Robo electrónico de fondos
- Pérdida de beneficios
- Extorsión cibernética (ransomware)
- Indemnización por responsabilidad civil ante terceros
- Asistencia jurídica

Avda. Manoteras, 24. Planta 2 – 28050 Madrid
T. 910 600 101 - M. info@datos101.com - W. www.datos101.com