

## **Los 10 dominios a implantar para evitar ciberataques según Hasten Group**

**El ciberespacio se ha convertido en el blanco perfecto para desarrollar una economía underground nutrida del robo de información y datos. Hasten Group señala las principales amenazas de las empresas y los 10 dominios de ciberseguridad a implantar en la estrategia de seguridad de la información**

Distancia y tiempo han sido eliminadas gracias al desarrollo de las tecnologías de la comunicación, un nuevo entorno donde imperan rapidez e inmediatez. La tecnología ocupa un papel relevante en cuanto a riesgos globales para los individuos (el 55% de los habitantes del planeta se relaciona por internet), los gobiernos y las empresas. El ciberespacio se ha convertido en un lugar activo “rentable” de amenazas en el que ha encontrado un hueco la economía underground basada en acciones ilícitas que se nutre del robo de información y datos. Las empresas se convierten en un blanco de posibles ataques al disponer de información privilegiada o confidencial.

Las principales amenazas a las que se enfrentan las empresas, según señala Hasten Group son la interrupción de servicios, esta interrupción conlleva la falta temporal de información intencionada. El sabotaje es otro de los peligros que conlleva deterioro intencionado o destrucción a largo plazo de la disponibilidad de la información. Un riesgo más, la manipulación de la información provoca la alteración intencionada de la información, con la consecuente pérdida de su integridad. Otro, el robo de información mediante copiado o eliminación de la información y que afecta a su confidencialidad. El espionaje protagonizado casi siempre por actores estatales o patrocinados por Estados que copian o eliminan información. La manipulación de sistemas a través de acciones de deterioro de sistemas o servicios de información, orientadas a atacar la confidencialidad o integridad y pudiéndose utilizar para llevar a cabo otros ataques. Y por último, las amenazas más complejas y multidimensionales denominadas amenazas híbridas que utilizan el ciberespacio como herramienta para realizar sus propósitos, estas son acciones coordinadas y sincronizadas que atacan deliberadamente vulnerabilidades sistémicas (capacidad para explotar los umbrales de detección y atribución de tales acciones).

Los ciberataques más utilizados siguen siendo, en un 90%, la propagación de código dañino a través de correos electrónicos que contienen carga dañina. De la misma manera el phishing que ha mejorado debido innovaciones constantes convenciendo a los usuarios de la autenticidad de las estafas, y ha entrado en escena una amenaza emergente de internet vinculada con la monetización directa: el cryptojacking o cryptomining denominada minería de criptomonedas maliciosa que se oculta en un ordenador o en un dispositivo móvil que utiliza sus recursos de la máquina para “extraer” criptomonedas.

Las empresas deben implementar soluciones de prevención de amenazas para evitar el robo. La seguridad de la información no puede comprarse hay que construirlas. Se caracteriza por la preservación de la confidencialidad, integridad y disponibilidad de la información; así como por su autenticación, responsabilidad y fiabilidad. La seguridad en la red debe ser entendida como una estrategia en un sentido amplio y es consecuencia de las interrelaciones existentes en las empresas

compuesta por 10 dominios de ciberseguridad distribuidos en 3 Procesos, Sistemas y Personas.

Los requisitos necesarios para implantar, mantener y mejorar un sistema de gestión de la seguridad de la información en los procesos son: políticas de seguridad de la información, establecer claramente las restricciones y comportamientos de los miembros, seguir protocolo de acceso a datos e indicar quien puede acceder a los mismos, relación con los proveedores y cumplimiento legal determinante que señala el proceso de garantías con los cumplimientos de la normativa y regulaciones en materia de seguridad informática. En los sistemas se implantarán los siguientes dominios: gestión de los incidentes de seguridad, la empresa debe anticiparse y prever su respuesta ante violaciones de seguridad informática; control de acceso, definiendo la restricción de los derechos de acceso a la información, redes o sistemas, adquisición desarrollo y mantenimiento, se detalla la integración de la seguridad en las aplicaciones, seguridad física, medioambiental, seguridad operacional a través de protección adecuada de las de las instalaciones informáticas dentro de una organización, gestión de las operaciones y comunicaciones, estableciendo la administración de los controles de seguridad técnica en los sistemas y las redes, gestión de activos, a través de un inventario y el esquema de clasificación para los recursos de información. En cuanto a las personas los dominios son dos: la seguridad recursos humanos que abordará cuales son los procedimientos de seguridad con los nuevos empleados, los que se desplazan y quienes dejan la empresa y la organización seguridad información a través de un modelo de gestión establecido por una organización para la seguridad de la información.

Los dominios, afirman en Hasten Group son los cimientos para desarrollar y llevar a cabo medidas estándares eficaces en materia de privacidad y seguridad empresarial.

Hasten Group: Consultora española, que nace en 2015, fruto de la fusión por absorción de dos empresas tecnológicas que reunían más 10 años de experiencia en el campo del desarrollo de aplicaciones móviles y web, con el objetivo de consolidarse como proveedor de confianza de servicios tecnológicos para empresas. Actualmente, cuenta con más de 100 profesionales. Ha participado en más 60 proyectos desarrollando su actividad en diferentes sectores: finanzas, telecomunicaciones, utilities, administración pública, sanidad, energía, formación o turismo. Está homologada por las más importantes multinacionales tecnológicas y financieras y representa un nuevo concepto en la búsqueda de la “especialización integrada” apostando por la eficiencia en profesionalización y gestión. <https://www.grupohasten.com>

**Datos de contacto:**

En Ke Medio Broadcasting  
912792470

Nota de prensa publicada en: [Madrid](#)

Categorías: [Nacional Finanzas Marketing Programación Hardware E-Commerce Ciberseguridad](#)

---

**NotasdePrensa**

<https://www.notasdeprensa.es>