GRUPOSIL INFORMÁTICA

Bitdefender

Global Leader
In Cybersecurity

FORMACIÓN DEL SOFTWARE DE SEGURIDAD DE BITDEFENDER

KIT DIGITAL

Financiado por la Unión Europea
NextGenerationEU

red.es

Plan de Recuperación, Transformación y Resiliencia

KIT DIGITAL

Contenido

Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

KIT DIGITAL

1. ¿Que es Bitdefener?

Bitdefender es una de las empresas líderes en seguridad cibernética a nivel mundial. Ofrece soluciones avanzadas para la protección contra diversas amenazas en dispositivos personales y redes corporativas. La empresa ha desarrollado una suite de productos diseñada para prevenir, detectar y eliminar una amplia gama de riesgos digitales que afectan a usuarios de todos los niveles. Entre las amenazas que combate se incluyen:

- Virus: Programas maliciosos diseñados para corromper archivos o sistemas.
- Malware: Software dañino que afecta al rendimiento y seguridad del dispositivo.
- Ransomware: Tipo de malware que bloquea archivos o sistemas y exige un pago para liberarlos.
- Phishing: Tácticas fraudulentas para obtener información personal mediante engaños, como correos electrónicos o sitios web falsificados.

La compañía integra múltiples tecnologías de seguridad en tiempo real, lo que asegura que los dispositivos estén protegidos constantemente frente a cualquier tipo de ciberataque. Bitdefender no solo ofrece software antivirus, sino también una gama más amplia de soluciones, como firewall, herramientas de control parental, protección para redes Wi-Fi y más.

1.1 Objetivo del Manual

Este documento tiene como finalidad proporcionar una guía detallada sobre el uso del software de seguridad **Bitdefender**. Su propósito es garantizar la correcta utilización de la herramienta, asegurando la protección del entorno digital de los usuarios sin acceso de administrador.

1.2 Importancia de la Ciberseguridad en el Entorno Profesional

En el entorno profesional actual, la ciberseguridad se ha convertido en un pilar fundamental para garantizar la integridad de la información y la operatividad de las empresas. La digitalización de los procesos empresariales ha traído consigo numerosos beneficios, pero también ha incrementado la exposición a amenazas cibernéticas que pueden comprometer la seguridad de los sistemas y la privacidad de los datos.

Los ataques cibernéticos han evolucionado en sofisticación y frecuencia, afectando tanto a grandes corporaciones como a pequeñas y medianas empresas. La filtración de datos, el robo de información confidencial y el secuestro de sistemas mediante ransomware son solo algunas de las amenazas a las que se enfrentan las organizaciones diariamente.

En este contexto, la implementación de medidas de ciberseguridad se ha vuelto imprescindible para minimizar riesgos y garantizar la continuidad del negocio.

Una estrategia efectiva de ciberseguridad comienza con la prevención. La adopción de soluciones de seguridad como Bitdefender permite identificar y mitigar amenazas antes de que estas causen daños irreparables. La protección en tiempo real contra malware, ransomware y ataques de phishing es esencial para resguardar la integridad de los sistemas informáticos. Además, el filtrado de contenido malicioso y la detección de vulnerabilidades fortalecen la postura de seguridad de la empresa.

Otro aspecto clave en la ciberseguridad es la concienciación y formación de los empleados. La ingeniería social sigue siendo una de las tácticas más utilizadas por los ciberdelincuentes para obtener acceso a información sensible.

Por ello, es crucial capacitar al personal en buenas prácticas de seguridad, como la gestión adecuada de contraseñas, el reconocimiento de correos electrónicos fraudulentos y la correcta manipulación de datos confidenciales.

La normativa y cumplimiento de estándares de seguridad también juegan un papel determinante en la protección de los entornos empresariales. Organismos como la Unión Europea han establecido regulaciones como el Reglamento General de Protección de Datos (GDPR), que exige a las empresas implementar medidas adecuadas para proteger la información de sus clientes y empleados. Cumplir con estos requerimientos no solo evita sanciones legales, sino que también refuerza la confianza de los clientes en la organización.

La monitorización y respuesta ante incidentes de seguridad es otro componente esencial dentro de un enfoque integral de ciberseguridad. La capacidad de detectar actividades sospechosas en tiempo real y reaccionar de manera inmediata permite mitigar los impactos de posibles ataques. Bitdefender proporciona herramientas avanzadas de monitoreo que analizan el tráfico de red, identifican patrones de comportamiento malicioso y alertan sobre cualquier intento de intrusión.

Además de las amenazas externas, las organizaciones deben considerar los riesgos internos. La fuga de información por parte de empleados malintencionados o negligentes representa una vulnerabilidad significativa. Implementar controles de acceso, cifrado de datos y políticas de seguridad rigurosas contribuye a minimizar estos riesgos y proteger los activos digitales de la empresa.

La evolución de la tecnología también ha traído consigo nuevos desafíos en el ámbito de la ciberseguridad. La adopción de entornos en la nube, el teletrabajo y el uso de dispositivos móviles han ampliado la superficie de ataque de las organizaciones.

Financiado por la Unión Europea NextGenerationEU

En este sentido, es fundamental contar con soluciones de seguridad adaptadas a estos nuevos escenarios, permitiendo una protección integral sin importar la ubicación de los usuarios o la infraestructura utilizada.

En conclusión, la ciberseguridad es un elemento crítico en el entorno profesional que no puede ser pasado por alto. La implementación de soluciones de seguridad robustas, junto con la concienciación y formación de los empleados, el cumplimiento de normativas y la monitorización continua, conforman un ecosistema de protección eficaz contra las amenazas cibernéticas.

Bitdefender, como herramienta avanzada de ciberseguridad, proporciona las capacidades necesarias para garantizar un entorno digital seguro, protegiendo tanto a empresas como a sus usuarios de los crecientes riesgos en el panorama digital actual.

2. Arquitectura de Bitdefener

La arquitectura de Bitdefender se organiza de manera que maximice la protección sin sobrecargar los dispositivos. Los componentes clave de su arquitectura incluyen:

- Agente local: Es un software instalado directamente en el dispositivo del usuario. Este agente realiza tareas como escanear archivos y procesos, detectar malware en tiempo real y defender contra ataques, entre otras funciones. Se encarga de la protección activa, proporcionando respuestas rápidas frente a posibles amenazas.
- Servidor central: Este servidor gestiona a todos los agentes locales en una red, manteniéndolos actualizados con las últimas definiciones de virus y patrones de amenazas. Además, permite realizar análisis globales, monitoreando el comportamiento de los agentes y generando informes sobre su actividad.
- Base de datos de amenazas: Contiene información detallada sobre amenazas conocidas (virus, malware, vulnerabilidades, etc.). Esta base de datos es actualizada regularmente para asegurarse de que el software esté al tanto de las amenazas emergentes y pueda reconocerlas de inmediato.

3. Función Operativa de Bitdefender

Bitdefender no se limita a ser una simple solución reactiva contra virus, sino que emplea **tecnologías avanzadas** para anticiparse y bloquear amenazas desconocidas. Esto lo consigue utilizando inteligencia artificial, análisis de comportamientos y la computación en la **nube** para obtener datos rápidos y precisos sobre posibles amenazas. Entre sus métodos de protección destacan:

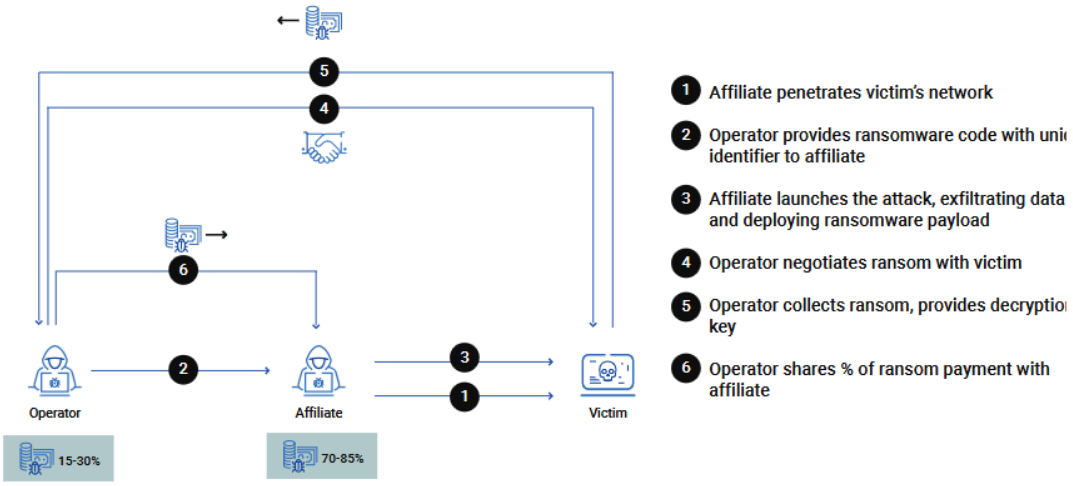
- **Detección heurística**: Analiza el comportamiento de los programas para identificar posibles amenazas que aún no han sido detectadas por las bases de datos tradicionales.
- **Análisis de tráfico de datos**: Permite a Bitdefender identificar patrones anormales en el tráfico de red y detectar ataques en curso, como los ataques de denegación de servicio (DDoS).
- **Aprendizaje automático**: Utiliza algoritmos que mejoran continuamente el software, lo que permite identificar amenazas más complejas o innovadoras.

4. El Agente de Bitdefender y sus Comunicaciones

El **agente local** es el componente esencial que reside en cada dispositivo protegido. Este agente mantiene una **comunicación constante** con el servidor central para garantizar que el dispositivo esté siempre actualizado con las últimas definiciones de amenazas y parches de seguridad.

Las **comunicaciones** entre el agente y el servidor se producen de la siguiente manera:

- **Actualizaciones de definiciones de virus**: El agente se conecta al servidor para descargar las últimas bases de datos de amenazas, lo que le permite identificar nuevos virus, malware y otras amenazas.
- **Envío de información sobre amenazas**: El agente informa sobre los resultados de los escaneos y alerta al servidor sobre posibles amenazas. Si se detecta un archivo o comportamiento sospechoso, el agente envía esta información al servidor para su evaluación.
- **Análisis en la nube**: Cuando el agente detecta una amenaza potencialmente desconocida, puede remitir al servidor a un sistema de análisis basado en la nube para examinar el archivo o proceso con mayor detalle, utilizando recursos más potentes para el análisis.
- **Mejoras continuas**: La retroalimentación de los agentes se utiliza para mejorar la protección, ya que los datos recopilados de millones de dispositivos permiten a Bitdefender identificar nuevas amenazas y actualizaciones de manera eficiente.



5. Componentes principales

5.1. Antivirus y Antimalware

Este componente es el corazón de Bitdefender. Se encarga de detectar, bloquear y eliminar virus, malware, troyanos, spyware, y otras amenazas. Utiliza varias técnicas de detección, como:

- **Análisis de firmas**: Identificación de virus conocidos a través de su código.
- **Análisis heurístico**: Detecta amenazas desconocidas al analizar el comportamiento de los archivos y programas.
- **Detección en la nube**: Recurre a una base de datos en la nube para obtener información actualizada sobre nuevas amenazas.

5.2. Firewall

El **firewall** actúa como una barrera entre tu dispositivo y las redes externas, protegiéndolo de accesos no autorizados y ataques de red. Algunas de sus funciones incluyen:

- **Filtrado de tráfico**: Bloquea conexiones sospechosas y permite solo el tráfico legítimo.
- **Protección contra ataques de red**: Previene ataques como los de denegación de servicio (DDoS).
- **Control de aplicaciones**: Permite configurar qué aplicaciones tienen acceso a la red.

5.3. Protección contra Ransomware

El **ransomware** es uno de los tipos de malware más peligrosos, ya que cifra tus archivos y exige un rescate para liberarlos. Bitdefender tiene un sistema de protección especializado que:

- **Bloquea la ejecución de ransomware**: Detecta el comportamiento típico del ransomware e impide que cifre tus archivos.
- **Copia de seguridad en tiempo real**: Si el ransomware cifra archivos, se pueden restaurar desde copias de seguridad previas sin perder información.

5.4. Antispam y Antiphishing

- **Antispam**: Filtra los correos electrónicos no deseados, bloqueando los que provienen de fuentes desconocidas o que intentan realizar actividades fraudulentas.
- **Antiphishing**: Protege al usuario de correos electrónicos y sitios web que intentan robar información confidencial, como contraseñas y datos bancarios. Detecta intentos de fraude y bloquea páginas de phishing.

5.5. Protección Web (Web Protection)

Este componente bloquea sitios web maliciosos, como aquellos que intentan infectar el dispositivo con malware o robar información personal. Se encarga de:

- **Bloqueo de sitios peligrosos**: Filtra sitios web de phishing, malware y otros peligros.
- **Protección en tiempo real**: Analiza el tráfico web para detectar amenazas a medida que navegas.

5.6. VPN (Red Privada Virtual)

Bitdefender incluye una **VPN** que cifra tu conexión a Internet y protege tu privacidad en línea. Sus funciones son:

- **Cifrado de tráfico**: Protege tus datos personales y navegación al encriptar la conexión a Internet.
- **Acceso seguro a redes Wi-Fi públicas**: Protege tus comunicaciones cuando te conectas a redes Wi-Fi abiertas, como en cafeterías o aeropuertos.
- **Navegación anónima**: Oculta tu dirección IP para evitar rastreos de tu actividad en línea.

5.7. Modo de Juego y Bajo Impacto

Bitdefender incluye un **modo de juego** que optimiza el rendimiento del sistema para que puedas jugar sin interrupciones. Al activar este modo:

- **Reducir el uso de recursos**: Minimiza el impacto en el rendimiento del sistema, liberando recursos para los juegos.
- **Desactivar notificaciones**: Evita que las notificaciones o alertas del antivirus interrumpan la experiencia de juego.

5.8. Protección de la Privacidad (Anti-tracking)

Este componente bloquea el **rastreo en línea** y protege tu información personal de los sitios web que intentan recolectar datos sin tu permiso:

- **Bloqueo de cookies**: Impide que sitios web rastreen tu actividad mediante cookies.
- **Protección contra rastreadores**: Detiene la recolección de datos de terceros mientras navegas.

5.9. Control Parental

Bitdefender también ofrece herramientas para padres que desean supervisar y limitar el uso de Internet por parte de sus hijos. Algunas de sus funciones son:

- **Filtrado de contenido web**: Bloquea el acceso a sitios web no apropiados según las categorías establecidas.
- **Límites de tiempo**: Establece límites en el tiempo de uso de Internet y aplicaciones.
- **Monitoreo de actividades**: Permite ver qué sitios web visitan los niños y qué aplicaciones utilizan.

5.10. Protección en la Nube

Bitdefender utiliza **análisis en la nube** para detectar amenazas más rápidamente. La nube permite realizar análisis avanzados sin sobrecargar los recursos locales del dispositivo. Este sistema ayuda a:

- **Detectar amenazas desconocidas**: Analiza archivos en la nube utilizando poderosos algoritmos de IA.
- **Recibir actualizaciones constantes**: Bitdefender puede obtener información de amenazas emergentes desde la nube para mantener su protección al día.

5.11. Sistema de Actualización Automática

Bitdefender se actualiza automáticamente para asegurarse de que siempre esté protegido contra las últimas amenazas. Esto incluye:

- **Actualizaciones de definiciones de virus**: Garantiza que el software siempre esté al tanto de las amenazas más recientes.
- **Actualización de bases de datos en tiempo real**: Permite recibir mejoras en las capacidades de detección y respuesta frente a nuevas amenazas.

5.12. Seguridad en la Nube

Bitdefender también ofrece capacidades de seguridad a nivel de red a través de la **plataforma de protección en la nube**. Esto permite:

- **Filtrar el tráfico**: Analizar el tráfico de red en tiempo real y prevenir ataques antes de que lleguen al dispositivo.
- **Detección avanzada de amenazas**: La inteligencia colectiva ayuda a identificar ataques a través de múltiples dispositivos.

6. Ciclo de Protección Adaptativa

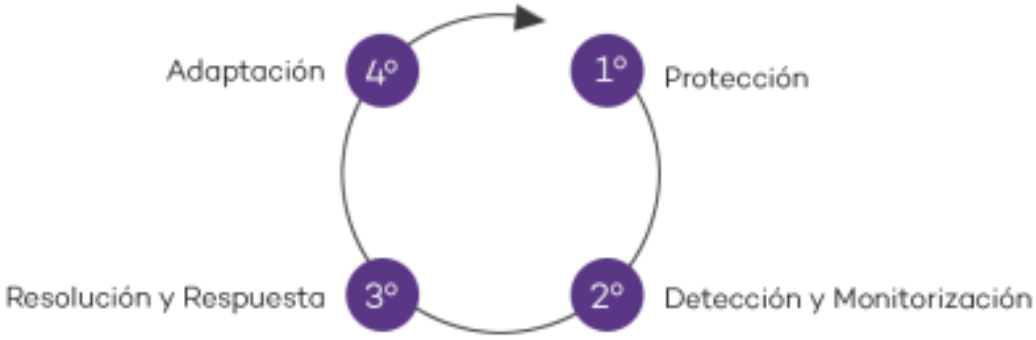
El **Ciclo de Protección Adaptativa** de Bitdefender es un enfoque integral y dinámico diseñado para enfrentar las amenazas cibernéticas de manera continua y proactiva. En lugar de ser un sistema que solo reacciona cuando ya ocurre un ataque, este ciclo se adapta, evoluciona y mejora constantemente, ofreciendo una protección avanzada frente a amenazas emergentes. Está basado en una combinación de tecnologías innovadoras, como inteligencia artificial, aprendizaje automático, análisis en la nube y detección comportamental.

El ciclo no es un proceso único, sino **circular y continuo**. Es decir, después de que el sistema pasa por la fase de adaptación, vuelve a la fase de detección y vuelve a empezar el ciclo, siempre mejorando y protegiendo de manera más eficaz frente a las amenazas cibernéticas.

Este ciclo se asegura de que el sistema esté siempre actualizado, que las amenazas sean detectadas antes de que causen daño y que cualquier ataque que logre superar las barreras sea mitigado de forma efectiva.

El ciclo consta de las siguientes etapas:

1. **Detección**: Identificación de amenazas conocidas y desconocidas mediante tecnologías avanzadas.
2. **Prevención**: Bloqueo proactivo de amenazas antes de que puedan ejecutarse.
3. **Respuesta**: Eliminación rápida de amenazas y restauración de archivos.
4. **Adaptación**: Aprendizaje de nuevas amenazas y ajustes automáticos para mejorar la protección.



7. Guía de instalación de Bitdefender

¿A quién va dirigida la guía de instalación? El objetivo es enseñar a través de unos pasos sencillos, cómo instalar Bitdefender y aprender cómo sacar partido a la solución siguiendo prácticas muy concretas.

Sigue los siguientes pasos que se indican a continuación y aprende a instalar y configurar Bitdefender para sacarle el máximo provecho. Recuerda que si tienes dudas durante el proceso siempre puedes contactar con nuestros expertos.

Paso 1 - Instalación de Bitdefender

Antes de continuar con la instalación, debe aceptar el Acuerdo de suscripción. Le recomendamos que dedique un momento a leerlo, ya que contiene los términos y condiciones bajo los cuales puede usar Bitdefender Internet Security. Si no está de acuerdo con estos términos, cierre la ventana. En ese caso, se cancelará el proceso de instalación y se cerrará el programa de instalación.

En este paso, tiene dos opciones adicionales:
❍ Mantener habilitada la opción *Enviar informes del producto*. Al activar esta opción, los informes que contienen datos sobre cómo utiliza el producto se envían a los servidores de Bitdefender. Esta información es esencial para mejorar el producto y nos

ayudará a ofrecerle una mejor experiencia en el futuro. Tenga en cuenta que estos informes no contienen datos confidenciales, como su nombre o dirección IP, y no se utilizarán con fines comerciales.

❍ Seleccionar el idioma en el que desea que se instale el producto.

Haga clic en *INSTALAR* para comenzar el proceso de instalación de su producto Bitdefender.

Paso 2 - Instalación en proceso

Espere a que se complete la instalación. Se mostrará información detallada sobre el progreso.

Paso 3 - Instalación completada

Una vez finalizada la instalación, se mostrará un resumen. Si durante el proceso se detectó y eliminó alguna amenaza activa, puede ser necesario reiniciar su sistema.

Paso 4 - Análisis del dispositivo

Ahora se le preguntará si desea realizar un análisis de su dispositivo para asegurarse de que esté seguro. Durante este paso, Bitdefender analizará las áreas críticas del sistema. Haga clic en *Iniciar análisis del dispositivo* para comenzar.

Puede ocultar la interfaz de análisis haciendo clic en *Ejecutar análisis en segundo plano*. Después, elija si desea recibir notificaciones cuando termine el análisis.

Cuando el análisis haya finalizado, haga clic en *Pasar a Crear cuenta*. Nota: Si no desea realizar el análisis, puede hacer clic en *Saltar*.

Paso 5 - Cuenta de Bitdefender

Tras completar la configuración inicial, aparecerá la ventana de *Cuenta de Bitdefender*. Es necesaria una cuenta Bitdefender para activar el producto y utilizar sus características en línea. Para más información, consulte la sección de *Bitdefender Central* (página 31).

Dependiendo de su situación, realice lo siguiente:

❍ *Quiero crear una cuenta de Bitdefender*:

Introduzca la información solicitada en los campos correspondientes. Los datos que ingrese serán confidenciales. La contraseña debe tener al menos ocho caracteres, incluir al menos un número o símbolo y contener tanto mayúsculas como minúsculas.

Antes de continuar, debe aceptar los *Términos de uso*. Lea detenidamente los términos y condiciones para el uso de Bitdefender. También puede acceder a la *Política de privacidad* para leerla.

Haga clic en *CREAR CUENTA*.

Nota: Una vez creada la cuenta, podrá utilizar la dirección de correo electrónico y la contraseña proporcionada para iniciar sesión en su cuenta a través de https://central.bitdefender.com o en la aplicación *Bitdefender Central*, siempre que esté instalada en uno de sus dispositivos Android o iOS.

❍ *Ya tengo una cuenta de Bitdefender*:

Haga clic en *Iniciar sesión*.

Introduzca su dirección de correo electrónico y haga clic en *SIGUIENTE*.

Ingrese su contraseña y haga clic en *INICIAR SESIÓN*.

Si olvidó su contraseña o desea cambiarla, siga estos pasos:
a. Haga clic en *¿Olvidó la contraseña?*
b. Ingrese su dirección de correo electrónico y haga clic en *SIGUIENTE*.
c. Revise su bandeja de entrada, copie el código de seguridad recibido y haga clic en *SIGUIENTE*.
d. Escriba la nueva contraseña y haga clic en *GUARDAR*.

Nota: Si tiene una cuenta de MyBitdefender, puede utilizarla para acceder a su cuenta de Bitdefender. Si olvidó su contraseña, primero debe restablecerla en https://my.bitdefender.com y luego utilizar las credenciales actualizadas para iniciar sesión en su cuenta de Bitdefender.

❍ *Quiero iniciar sesión con mi cuenta de Microsoft, Facebook o Google*:

Seleccione el servicio que desea utilizar. Será redirigido a la página de inicio de sesión de ese servicio.

Siga las instrucciones del servicio elegido para vincular su cuenta a Bitdefender.

Nota: Bitdefender no tiene acceso a información confidencial, como las contraseñas de las cuentas con las que se conecta, ni a los datos personales de sus amigos y contactos.

Paso 6 - Activación del producto

Nota: Este paso se muestra si ha creado una cuenta Bitdefender nueva durante el paso anterior o si inició sesión con una cuenta cuya suscripción ha caducado. Es necesario estar conectado a Internet para completar la activación de su producto. Dependiendo de su situación, proceda de la siguiente manera:

❍ *Tengo un código de activación*:

Ingrese el código de activación en el campo *Tengo un código de activación* y haga clic en *CONTINUAR*.
Nota: El código de activación se encuentra en la etiqueta del CD/DVD, la tarjeta de licencia del producto o en el mensaje de confirmación de compra online.

❍ *Quiero evaluar Bitdefender*:

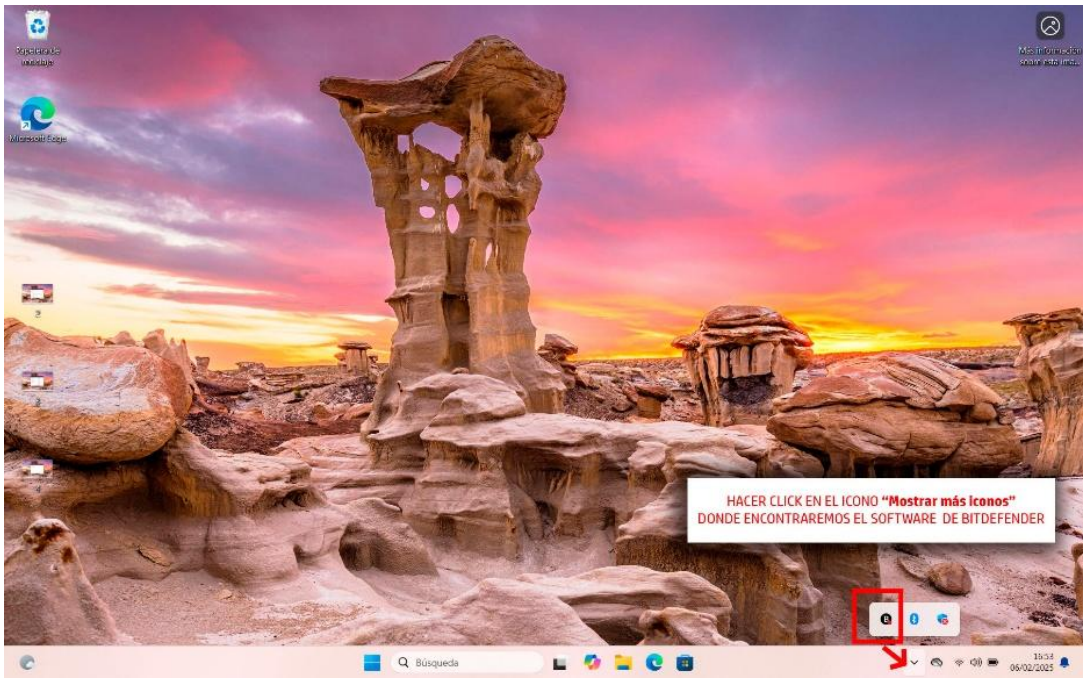
En este caso, puede utilizar el producto durante un período de treinta días. Para comenzar el período de evaluación, seleccione *No tengo ninguna suscripción; quiero probar el producto gratuitamente* y haga clic en *CONTINUAR*.

Paso 7 - Primeros pasos

En la ventana *Primeros pasos* podrá ver la información relacionada con su suscripción activa.
Haga clic en *FINALIZAR* para acceder a la interfaz de *Bitdefender Internet Security*.

8. Interfaz y Funcionalidades Principales para el usuario

8.1 Acceso al Software de Seguridad de Bitdefender

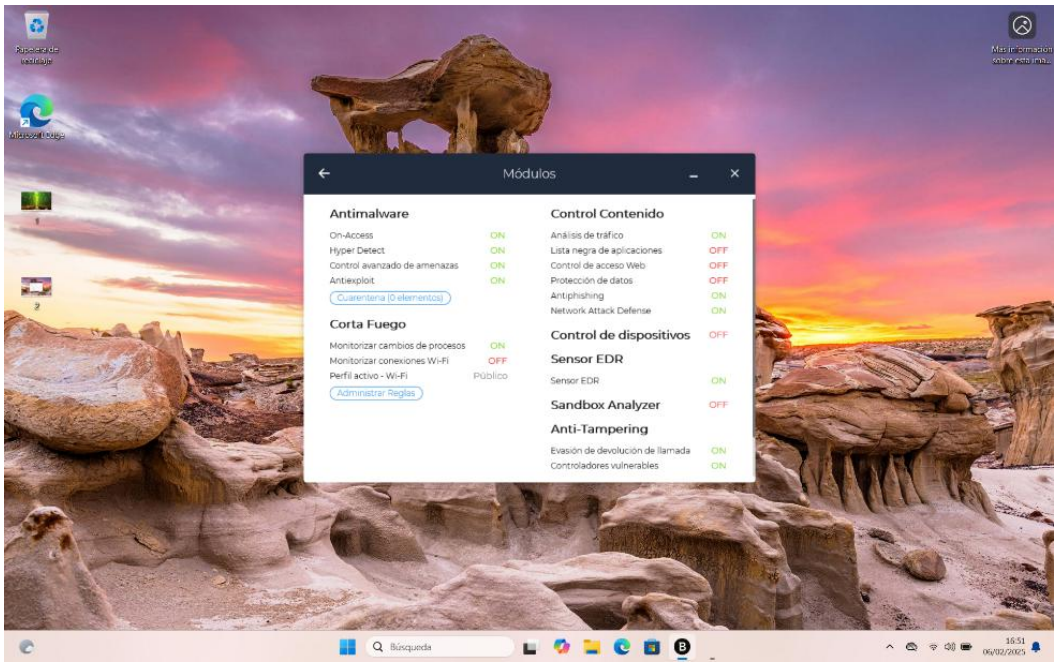


8.2 Panel de Control

El panel principal te informa sobre eventos de seguridad y problemas en la actualización de Bitdefender, indicando que el sistema podría estar en riesgo. Es recomendable revisar y solucionar las incidencias para garantizar la protección del equipo.

8.3 Menú Principal y Navegación

En la siguiente pantalla se muestra un módulo de seguridad informática que incluye varias funciones relacionadas con la protección del sistema. Te explico cada una de ellas:



8.3.1. Antimalware

Estas funciones protegen el sistema contra amenazas como virus, malware y exploits.

- **On-Access**: El antivirus analiza los archivos en tiempo real cuando se abren o modifican.
- **Hyper Detect**: Detecta amenazas avanzadas y ataques antes de que se ejecuten.
- **Control avanzado de amenazas**: Ofrece protección contra amenazas persistentes avanzadas (APT).
- **Antiexploit**: Previene ataques que explotan vulnerabilidades en software.
- **Cuarentena**: Sección donde se almacenan archivos sospechosos para evitar daños.

8.3.2. Cortafuego (Firewall)

Controla y supervisa el tráfico de red para prevenir accesos no autorizados.

- **Monitorizar cambios de procesos**: Detecta modificaciones en procesos activos, evitando ataques como inyecciones de código.
- **Monitorizar conexiones Wi-Fi**: Supervisa la seguridad de las redes Wi-Fi (desactivado en la imagen).
- **Perfil activo**: Indica el tipo de conexión (Wi-Fi en este caso).
- **Administrar reglas**: Permite configurar reglas de firewall.

8.3.3. Control de Contenido

Regula el acceso a información y sitios web.

- **Análisis de tráfico**: Examina el tráfico de red para detectar actividades sospechosas.
- **Lista negra de aplicaciones**: Bloquea la ejecución de programas no autorizados (desactivado).
- **Control de acceso Web**: Restringe el acceso a sitios no permitidos (desactivado).
- **Protección de datos**: Evita el robo o filtración de datos sensibles (desactivado).
- **Antiphishing**: Detecta y bloquea intentos de robo de credenciales mediante sitios web falsos.
- **Network Attack Defense**: Defiende contra ataques en la red.

8.3.4. Control de Dispositivos

Impide la conexión de dispositivos no autorizados (desactivado en la imagen).

8.3.5. Sensor EDR (Endpoint Detection and Response)

- **Sensor EDR**: Monitorea en tiempo real actividades sospechosas en el sistema.

8.3.6. Sandbox Analyzer

Permite ejecutar archivos en un entorno aislado para verificar si contienen malware (desactivado).

8.3.7. Anti-Tampering

Protege el sistema contra intentos de manipulación de seguridad.

- **Evasión de devolución de llamada**: Evita técnicas de evasión utilizadas por malware.
- **Controladores vulnerables**: Protege contra ataques que explotan controladores inseguros.

9. Política de Seguridad Requerida por Red.es

Para que un equipo cumpla con las condiciones de ciberseguridad mínimas y sea subvencionable bajo el programa **Kit Digital**, debe contar con las siguientes políticas de seguridad:

- **Antimalware**: Análisis de memoria interna y dispositivos de almacenamiento externos.
- **Antispyware**: Detección y prevención de malware espía.
- **Correo Seguro**: Antispam y antiphishing para proteger los correos electrónicos.
- **Navegación Segura**: Control de contenidos y bloqueo de anuncios maliciosos.
- **Análisis y Detección de Amenazas**: Identificación y mitigación de amenazas nuevas y conocidas.
- **Monitorización de la Red**: Supervisión del tráfico y alertas ante intrusiones.
- **Configuración y Actualizaciones**: Implementación de configuraciones seguras y aplicación de actualizaciones regulares.

10. Resolución de Problemas

10.1 Errores Comunes y Soluciones

- **Bitdefender no se ejecuta**: Reinicie el equipo y verifique el estado de la licencia.
- **Alertas de seguridad constantes**: Compruebe si hay conflictos con otro software de seguridad.
- **Problemas de acceso a programas**: Puede tratarse de una amenaza bloqueada. Contacte con soporte técnico.

10.2 Optimización del Rendimiento

Para mejorar el desempeño del equipo, se recomienda:

- Mantener Bitdefender actualizado.
- Ejecutar escaneos de seguridad de forma regular.
- Evitar la instalación de software desconocido.

10.3 Restauración de Configuraciones Predeterminadas

Si el software presenta fallos, puede restaurarse la configuración inicial desde el menú de opciones avanzadas.

10.4 Contacto con Soporte Técnico

Para asistencia técnica, contacte con:

- **Correo Electrónico:** formacion@grupo-sil.com

11. Buenas Prácticas de Ciberseguridad

11.1 Consejos Generales

- Utilizar redes seguras y evitar conexiones públicas sin protección.
- Emplear contraseñas seguras y únicas para cada servicio.
- Activar la autenticación en dos pasos en todas las cuentas posibles.
- No compartir credenciales de acceso ni información confidencial con terceros.
- Descargar software únicamente de fuentes confiables y oficiales.

11.2 Actualizaciones y Mantenimiento

- Mantener Bitdefender actualizado para garantizar la protección ante nuevas amenazas.
- Realizar escaneos de seguridad de manera periódica.
- Aplicar actualizaciones de software y parches de seguridad en el sistema operativo.
- Configurar copias de seguridad automáticas para proteger la información clave.

11.3 Educación del Usuario

- Reconocer intentos de phishing y evitar hacer clic en enlaces sospechosos.
- No descargar archivos adjuntos de correos electrónicos de remitentes desconocidos.
- Capacitar a los empleados en buenas prácticas de ciberseguridad.
- Evitar el uso de dispositivos externos sin escanearlos previamente.

12. Preguntas Frecuentes (FAQ)

- **¿Una impresora puede generar conflictos con Bitdefender?**
  Sí, en algunos casos, Bitdefender puede bloquear el acceso de la impresora si detecta un posible riesgo de seguridad. Para solucionarlo, se recomienda agregar la dirección IP de la impresora a la lista de excepciones del firewall de Bitdefender. También se puede verificar la configuración del firewall para asegurarse de que no está bloqueando los puertos utilizados por la impresora.
- **Si me conecto con RJ45 a una intranet, ¿puede haber problemas de conexión con Bitdefender?**
  En algunos entornos corporativos, Bitdefender puede interferir con la conexión de red si detecta una posible amenaza en la intranet. Si experimenta problemas de conexión, verifique que Bitdefender no esté bloqueando la dirección IP de la intranet en la configuración del firewall. Además, consulte con el administrador del sistema para asegurarse de que la configuración de seguridad es compatible con la red interna.
- **¿Puedo pausar el uso de Bitdefender temporalmente?**
  No se recomienda desactivar Bitdefender por razones de seguridad, pero si es absolutamente necesario, los usuarios pueden desactivar temporalmente la

- protección en tiempo real desde la configuración del software. Sin embargo, esta opción puede estar restringida por el administrador del sistema en entornos corporativos. Para realizar esta acción, contacte con el equipo de soporte técnico.
- **Si un aplicativo no me deja acceder pero es de confianza, ¿cómo debo gestionarlo?**
  Si un programa legítimo está siendo bloqueado por Bitdefender, puede agregarse a la lista de exclusiones. Para ello, acceda a la configuración de Bitdefender, diríjase a la sección de "Excepciones" y agregue el ejecutable del programa. Es importante asegurarse de que la aplicación es confiable antes de realizar esta acción.
- **¿Cómo puedo abrir un puerto específico en Bitdefender?**
  Para abrir un puerto en el firewall de Bitdefender, acceda a la configuración del firewall, seleccione la opción de "Reglas", y agregue una nueva regla para permitir el tráfico en el puerto deseado. Se recomienda consultar con el administrador de TI antes de realizar esta acción para evitar riesgos de seguridad.
- **¿Cómo puedo conocer la dirección IP de un dispositivo externo para poder abrir un puerto?**
  Para identificar la dirección IP de un dispositivo externo, siga estos pasos:

  1. Si el dispositivo está en la misma red, puede verificar la configuración de su router accediendo a su panel de administración y revisando la lista de dispositivos conectados.
  2. En Windows, puede utilizar el comando arp -a en la terminal de comandos para ver una lista de dispositivos y sus direcciones IP asociadas.
  3. En macOS y Linux, el comando ping [nombre_del_dispositivo] o ifconfig (en Linux también ip a) puede ayudar a identificar direcciones IP de dispositivos en la red.
  4. Si el dispositivo está fuera de la red local, puede pedirle a su administrador de TI o consultar la documentación del servicio para obtener la IP externa asignada.
- **¿Una impresora puede generar conflictos con Bitdefender?**
  Sí, en algunos casos, Bitdefender puede bloquear el acceso de la impresora si detecta un posible riesgo de seguridad. Para solucionarlo, se recomienda agregar la dirección IP de la impresora a la lista de excepciones del firewall de

- Bitdefender. También se puede verificar la configuración del firewall para asegurarse de que no está bloqueando los puertos utilizados por la impresora.

- **Si me conecto con RJ45 a una intranet, ¿puede haber problemas de conexión con Bitdefender?**
  En algunos entornos corporativos, Bitdefender puede interferir con la conexión de red si detecta una posible amenaza en la intranet. Si experimenta problemas de conexión, verifique que Bitdefender no esté bloqueando la dirección IP de la intranet en la configuración del firewall. Además, consulte con el administrador del sistema para asegurarse de que la configuración de seguridad es compatible con la red interna.

- **¿Puedo pausar el uso de Bitdefender temporalmente?**
  No se recomienda desactivar Bitdefender por razones de seguridad, pero si es absolutamente necesario, los usuarios pueden desactivar temporalmente la protección en tiempo real desde la configuración del software. Sin embargo, esta opción puede estar restringida por el administrador del sistema en entornos corporativos. Para realizar esta acción, contacte con el equipo de soporte técnico.

- **Si un aplicativo no me deja acceder pero es de confianza, ¿cómo debo gestionarlo?**
  Si un programa legítimo está siendo bloqueado por Bitdefender, puede agregarse a la lista de exclusiones. Para ello, acceda a la configuración de Bitdefender, diríjase a la sección de "Excepciones" y agregue el ejecutable del programa. Es importante asegurarse de que la aplicación es confiable antes de realizar esta acción.

- **¿Cómo puedo abrir un puerto específico en Bitdefender?**
  Para abrir un puerto en el firewall de Bitdefender, acceda a la configuración del firewall, seleccione la opción de "Reglas", y agregue una nueva regla para permitir el tráfico en el puerto deseado. Se recomienda consultar con el administrador de TI antes de realizar esta acción para evitar riesgos de seguridad.

- **¿Cómo actualizo Bitdefender?**

  Se actualiza automáticamente, pero también puede hacerse manualmente desde la configuración.

- **¿Qué hacer si detecto una amenaza?**

  Permitir que Bitdefender elimine la amenaza y contactar con el soporte técnico.

- **¿Puedo desactivar Bitdefender temporalmente?**

  No se recomienda, pero puede ser administrado por el soporte técnico.

13. Formación en concienciación sobre la ciberseguridad

Indice

Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

¿Qué es la formación en conciencia de seguridad?

La capacitación en conciencia de seguridad es la forma más eficaz de proteger a las empresas y a sus empleados de los ataques de phishing de ingeniería social.Pero,

¿Qué es la formación en conciencia de seguridad?

Se define la capacitación en concientización sobre seguridad como un programa educativo que enseña a los empleados sobre seguridad y phishing mientras crea las mejores prácticas y buenos hábitos.

Una de las mayores debilidades de cualquier sistema de ciberseguridad es el factor humano. No importa si tu organización está usando contraseñas sofisticadas, múltiples firewalls, programas anti-malware, etc. El factor humano siempre será un problema para mantener a tu empresa a salvo.

Al final del día, los empleados son los más vulnerables y necesitan las herramientas adecuadas. Si un empleado no ha recibido una formación eficaz sobre la concienciación sobre la seguridad cibernética, es muy probable que comprometa a la empresa a través de simples errores, negligencia o incluso apatía.

Los ciberdelincuentes lo saben. Saben que el hardware es increíblemente difícil de conseguir, pero apuntar a una persona o grupo les da la mejor oportunidad de atacar. El uso de métodos como los correos electrónicos de phishing aprovecha las vulnerabilidades humanas. Cuando se usa con éxito, algo tan simple como un correo electrónico de phishing puede poner en peligro a toda una organización y su red.

Esas son malas noticias.

La formación en concienciación sobre ciberseguridad pretende resolver esto centrándose directamente en el factor humano.

Financiado por la Unión Europea NextGenerationEU

El objetivo es dejar al empleado no asustado, sino consciente. Sin miedo, pero un poco paranoico con los correos electrónicos.

El surgimiento de la seguridad psicológica

A medida que el panorama de las amenazas cibernéticas continúa creciendo, proteger nuestros sistemas de información se vuelve cada vez más difícil. A menudo, esto se debe a que el enfoque, la atención y, en última instancia, la culpa están en los lugares equivocados. Hemos comenzado a ver una necesidad de empresas más allá de la seguridad de la información, y la razón de esto está ahí en el nombre.

Proteger la información de una empresa simplemente concentrándose en la información en sí aún te deja vulnerable, ya que más del 90% de las infracciones involucran ingeniería social. Por loco que parezca, tenemos que proteger nuestras mentes, nuestras intuiciones, nuestra dependencia y nuestra confianza. Introduce la idea de la formación en conciencia de seguridad psicológica.

La seguridad psicológica es la práctica de proteger a los humanos de ser manipulados y explotados por la tecnología. Desde anuncios hiperdirigidos hasta ataques de phishing, la tecnología y los datos se utilizan para influir en nosotros todos los días. Esta es la razón por la que el phishing tiene tanto éxito. Hemos aprendido a confiar y depender de la tecnología que usamos, las marcas que compramos y las personas que conocemos.

Agrega el hecho de un entorno profesional con jefes, plazos y aumentos, y el riesgo de manipulación se dispara.

¿Te enamorarás de un correo electrónico de phishing de Starbucks? Quizás. ¿Descargarás una hoja de cálculo misteriosa de tu «jefe» llamada «ChristmasBonuses2020.xlsx»? Definitivamente.

Ésta es la razón por la que el entrenamiento regular es tan importante. Para protegernos contra el phishing, debemos capacitar a los empleados para que reconozcan el riesgo y creen un reconocimiento de patrones a lo largo del tiempo.

Beneficios de la capacitación en conciencia de seguridad

Iniciativas como la capacitación en concientización sobre seguridad cibernética obligan a una empresa a examinar sus procedimientos, políticas y personal. Las ineficiencias y oportunidades a menudo salen a la luz como resultado de esto, lo que puede no tener nada que ver con la seguridad, pero aun así puede beneficiar a una empresa.

La capacitación en conciencia de seguridad puede ayudar a reducir errores o ayudar a reconocer los trucos y tendencias de los «malos».

La capacitación en concienciación sobre ciberseguridad para empleados puede fortalecer y mejorar la postura de seguridad de tu empresa.

Cuando sus empleados están educados y capacitados, son más compatibles.

La capacitación puede mantener limpia la reputación de tu cliente y libre de contratiempos.

La educación y la formación pueden reforzar la confianza e incluso ayudar a la moral de tus clientes.

Puedes ahorrar dinero, tiempo y datos confidenciales para tu cliente al recibir capacitación.

Tu cliente puede dormir por la noche sabiendo que se estás entrenando activamente para afrontar las últimas amenazas a través de la formación.

Construyendo una cultura de conciencia de seguridad

Un programa de formación de concienciación sobre seguridad puede actuar como un ejercicio de colaboración y creación de equipos. Debido a que la naturaleza del objetivo generalmente no es resolver un problema donde sea común señalar con el dedo, se presta a mejorar las relaciones entre los empleados. Un enemigo común (amenazas cibernéticas) a menudo une a un grupo.

Cuando las empresas se dan cuenta de la importancia de la capacitación en concienciación sobre seguridad y adoptan un programa, aumentan la productividad, impulsan la creatividad y, en última instancia, son mucho más seguras.

Evolución de los ataques dirigidos a humanos

Phishing y malware

Entre las principales amenazas cibernéticas, el malware sigue siendo un peligro importante. El brote de WannaCry de 2017 que costó a las empresas de todo el mundo hasta $ 4 mil millones aún se encuentra en la memoria reciente, y a diario se descubren otras nuevas cepas de malware. El phishing también ha experimentado un resurgimiento en los últimos años, con muchas nuevas estafas que se han inventado para aprovecharse de empresas desprevenidas.

Trabajar desde casa

El personal que trabaja desde casa está fuera de la supervisión directa de los equipos de soporte de TI y, a menudo, tiene dificultades para hacer frente a las amenazas cibernéticas y proteger adecuadamente la información de la empresa.

No actualizar el software y los sistemas operativos, enviar datos a través de redes inseguras y aumentar la dependencia del correo electrónico y la mensajería en línea ha hecho que los empleados sean mucho más susceptibles a amenazas que van desde malware hasta phishing.

Error humano

Si bien las soluciones técnicas como los filtros de correo no deseado y los sistemas de administración de dispositivos móviles son importantes para proteger a los usuarios finales, con la cantidad de amenazas y la multitud de sistemas y comunicaciones a través de los cuales el personal realiza su trabajo, el único factor de riesgo unificador que debe abordarse para mejorar fundamentalmente la seguridad es el papel del error humano.

Casi todas las infracciones cibernéticas exitosas comparten una variable en común: el error humano. El error humano puede manifestarse de muchas formas: desde no instalar las actualizaciones de seguridad de software a tiempo hasta tener contraseñas débiles y ceder información confidencial a correos electrónicos de phishing.

A pesar de que el software moderno de detección de amenazas y anti-malware se ha vuelto más sofisticado, los ciberdelincuentes saben que la eficacia de las medidas técnicas de seguridad solo llega hasta donde las personas las utilizan correctamente. Si un ciberdelincuente logra adivinar la contraseña de un portal de empresa en línea, o utiliza la ingeniería social para que un empleado realice un pago a una cuenta bancaria controlada por el ciberdelincuente, no hay nada que las soluciones técnicas puedan hacer para detener esa intrusión.

Dado que el error humano juega un papel tan importante en las infracciones cibernéticas, abordarlo es clave para reducir las posibilidades de que tu empresa sea atacada con éxito. También te permite proteger tu empresa de una gama de amenazas mucho más amplia que la que podría ofrecer cualquier solución técnica. La mitigación del error humano debe ser clave para la seguridad cibernética empresarial.

¿Cuándo ocurre el error humano?

Deben estar presentes dos factores para que se manifieste el error humano:

Oportunidad

Decisión

Oportunidad significa que existe una situación en la que un humano puede cometer un error: por ejemplo, permitir que los usuarios finales manejen las actualizaciones de software en lugar de forzar las actualizaciones de seguridad con la administración de parches. La decisión es la acción del individuo: en este caso, la falta de acción en la instalación de actualizaciones de seguridad cuando están disponibles.

Un esfuerzo de mitigación integral incluye tanto la reducción de la posibilidad de error como la mejora de las decisiones tomadas por los usuarios finales. Actuar en ambas áreas es fundamental para garantizar que se aborde a fondo el error humano.

En el caso de la aplicación de parches, por ejemplo, una medida técnica como la introducción de la gestión de parches puede reducir la posibilidad de error humano al mínimo en la mayoría de los casos, pero sigue siendo esencial tener en cuenta las situaciones en las que las soluciones técnicas tienen un lapso temporal, o si se introduce una situación nueva, como una política BYOD, en la que los usuarios pueden utilizar sus propios dispositivos sin gestión de parches.

En otros casos, como con los correos electrónicos de phishing, las medidas técnicas como los filtros de correo no deseado y el software de detección de infracciones tienen un efecto muy limitado para reducir la posibilidad de error cuando se enfrenta a un ataque dirigido. Aquí, la única forma eficaz de mitigar el error humano es enseñar a los usuarios finales cómo hacer mejores juicios.

¿Cómo se puede reducir el error humano?

Para que los usuarios finales tomen el juicio correcto en una situación de seguridad, deben estar presentes cuatro factores diferentes.

Comprensión

El primero de ellos es bastante sencillo: el usuario debe reconocer que se encuentra en una situación en la que la seguridad está potencialmente en juego. Sin reconocer la situación como tal, es posible que el usuario ni siquiera se dé cuenta de que está tomando una decisión debido a su inacción.

Empoderamiento

En segundo lugar, el usuario debe saber cuál es el curso de acción correcto. Esto no requiere necesariamente que el usuario comprenda completamente la amenaza, pero a menudo es tan simple como informar de la situación a una persona del departamento de TI o de seguridad que pueda investigarla.

Educación

En tercer lugar, el usuario debe saber por qué es importante la seguridad, para que comprenda la importancia de no ignorar los procedimientos de seguridad y sea consciente de las posibles implicaciones de una infracción. Si bien estos tres factores son todos esenciales para mejorar los resultados de seguridad, es en este punto crucial donde las empresas suelen fallar. Para poder tomar mejores decisiones en situaciones del mundo real, el cuarto factor también debe entrar en juego.

Eliminar la evitación del dolor

Problemas como la seguridad débil de las contraseñas y la imposibilidad de parchear el software persisten en organizaciones de todo el mundo, a pesar de que muchos usuarios de computadoras comprenden por qué estos problemas son críticos para la seguridad. La razón por la que no se toman medidas a pesar del conocimiento se debe a lo que llamamos evitación del dolor. Tener una contraseña única y segura requiere más tiempo para crear y más esfuerzo para recordar que una contraseña corta, débil o reutilizada.

A pesar de que un usuario lo sabe mejor, este 'dolor' causado por la creación de una contraseña segura suele ser lo suficientemente fuerte como para hacer que el usuario vaya en contra de su mejor criterio. Esto se ve agravado por el hecho de que, a pesar de que muchos usuarios toman las medidas correctas en circunstancias óptimas, las situaciones de trabajo urgente y ajetreado, así como el estrés, pueden hacer que las medidas de seguridad se sientan aún más «dolorosas» para los usuarios.

Impulsar el cambio cultural

Es este último factor el que solo puede resolverse mediante el cambio cultural. Los usuarios finales deben sentir que el dolor causado por seguir las mejores prácticas de seguridad es menor que la satisfacción obtenida por no hacerlo.

Las medidas técnicas como los administradores de contraseñas son esenciales en esto, ya que facilitan mucho la actuación de forma segura: si los empleados no tienen que crear o recordar sus propias contraseñas, no tienen ninguna razón para no utilizar las seguras. Simultáneamente, el umbral para realizar la acción correcta debe reducirse mediante el cambio cultural. Esto significa poner la seguridad a la vanguardia de la toma de decisiones y garantizar que los usuarios nunca sientan que están «perdiendo el tiempo» tomando las precauciones de seguridad adecuadas.

La seguridad debe ser discutida entre los empleados, y las preguntas y los puntos que los usuarios finales plantean sobre los problemas de seguridad en sus propios roles deben ser atendidos y recompensados. Esto ayuda a los usuarios a sentir que la seguridad no es solo una ocurrencia tardía, sino algo en lo que siempre vale la pena dedicar tiempo.

Financiado por la Unión Europea NextGenerationEU

La capacitación efectiva en concientización sobre seguridad aborda no uno, sino los cuatro factores. Esto significa identificar situaciones en las que los datos o los sistemas podrían verse comprometidos, comprender las mejores prácticas, conocer las posibles consecuencias de las infracciones y, finalmente, ayudar a impulsar un cambio cultural para crear un entorno en el que las consideraciones de seguridad siempre se tengan en cuenta en la toma de decisiones.

Cómo abordar la seguridad en el trabajo desde casa

Los empleados que no estaban acostumbrados a trabajar desde casa antes de la pandemia descubrieron rápidamente algunos de los problemas que causaría: tener que cuidar a los niños y las mascotas, lidiar con la mala conectividad a Internet y soportar todas las demás molestias que pueden ocurrir en hogar. En medio de todos estos nuevos cambios en el entorno de trabajo, la seguridad con demasiada frecuencia cayó al final de las listas de prioridades de los usuarios.

Los usuarios finales que trabajan desde casa están fuera de la supervisión del departamento de soporte de TI y pueden tener problemas con problemas simples relacionados con la tecnología. No es de extrañar que los ciberdelincuentes no hayan desperdiciado ni un segundo aprovechando las circunstancias de la pandemia para crear nuevas formas de estafas y delitos cibernéticos.

El equipo de soporte de TI no puede estar en el hogar de todos los usuarios finales, por lo que es esencial asegurarse de que, además de tener el equipo adecuado, los usuarios finales sean conscientes de sus responsabilidades individuales para mantener la seguridad. Los usuarios finales deben saber que son responsables de garantizar que solo accedan a la información y las redes de la empresa en dispositivos y redes que estén actualizados y sean seguros.

La formación en conciencia de seguridad es clave para garantizar que los usuarios finales sepan cómo mantener la seguridad. Es mejor dividir el entrenamiento en componentes pequeños y digeribles, ya que esto asegura que los usuarios no se sientan abrumados.

La capacitación también debe realizarse con regularidad, una vez al mes, como mínimo, para garantizar que se conserve el aprendizaje clave y que los usuarios no se olviden de la seguridad tan pronto como llegue el próximo proyecto de trabajo que sacuda la lista de prioridades.

Por último, es importante probar a los usuarios finales. Debe quedar claro que esto no es para juzgar o penalizar a los usuarios que luchan con su capacitación, sino para identificar brechas de seguridad clave en la fuerza laboral y abordarlas antes de que puedan ser explotadas por los ciberdelincuentes.

¿Cuál es el mejor formato para la formación de concienciación sobre seguridad?

La capacitación en conciencia de seguridad no es todo lo mismo. La forma en que se realiza, estructura y presenta la formación tendrá un efecto importante en su eficacia para mejorar realmente los resultados de seguridad en tu organización. En esta sección, veremos cuál es exactamente la mejor manera de realizar una capacitación en conciencia de seguridad para los usuarios finales.

Entrenamiento de la vieja escuela vs moderno

La capacitación en conciencia de seguridad solía significar hacer que los usuarios finales se sentaran a través de una sesión anual que constaba de horas de conferencias y presentaciones de diapositivas. La idea era que los usuarios recordaran algo de lo que vieron y escucharon. Sin embargo, ¿hasta dónde llegó para mejorar realmente los resultados de seguridad? No funcionó y todo el mundo lo odió.

Hay varias razones por las que este tipo de formación anual basada en conferencias no es eficaz. La primera de ellas es que en una sesión de capacitación anual, simplemente habrá demasiada información a la vez para que cualquier empleado la asimile y la recuerde. Incluso si los usuarios reciben material de aprendizaje para que lo lleven consigo o se les envían recordatorios ocasionales, es probable que la mayor parte del material de la sesión de capacitación entre por un oído y salga por el otro, olvidado en unos momentos.

Las conferencias y las presentaciones de diapositivas simplemente no son formatos atractivos para que los usuarios finales aprendan. No logran despertar el interés de los empleados de la misma manera que lo hacen los videos y el contenido interactivo, y con demasiada frecuencia están llenos de información innecesaria que no es relevante para todos los usuarios finales. Las diapositivas con texto pequeño seguramente harán que cualquier empleado se quede dormido a la mitad de la sesión.

La última y principal razón por la que el entrenamiento tradicional no es efectivo es que no hace uso del aprendizaje a través de la repetición. Si hay un año entre las sesiones de aprendizaje, los usuarios simplemente no recordarán lo que han aprendido, y la conciencia de los problemas de seguridad en general se desplomará en

los días y semanas posteriores a la capacitación. La seguridad no puede ser algo único, sino que debe serlo todo el año para que sea eficaz.

La capacitación en concienciación sobre seguridad se ha desplazado cada vez más a soluciones de software como servicio en línea. La capacitación basada en la nube ofrece

algunos beneficios inmediatos sobre los métodos tradicionales, pero no es necesariamente la respuesta definitiva a la conciencia de seguridad a menos que se brinde en ciertas áreas que son esenciales para mejorar genuinamente los resultados de seguridad.

¿Cómo hacer que la formación sea realmente eficaz?

Es posible contar con un programa de formación de concienciación sobre seguridad realmente eficaz, pero hay algunos criterios importantes que debes seguir para involucrar realmente a tus usuarios.

Dividir el material

Existe una cantidad limitada de información que una persona puede absorber a la vez. Esto es especialmente cierto cuando se trata de temas sobre los que la mayoría de los empleados no tienen muchos conocimientos previos. Para que la cantidad de material de aprendizaje no abrume a los usuarios finales, debe dividirse adecuadamente en segmentos, cada uno con su propio mensaje claro y simple que se presenta a los usuarios de una manera fácilmente digerible.

Ejecutar entrenamiento regular

Otro beneficio de desglosar el material de aprendizaje es que permite que el aprendizaje sea continuo, en lugar de hacerlo una sola vez. Dividir el aprendizaje en partes permite que estas secciones se envíen con regularidad durante todo el año, lo que ayuda a mantener la conciencia de seguridad constantemente en la mente de los usuarios finales. Como la repetición es clave para el aprendizaje, esto es crucial para garantizar que los usuarios recuerden realmente lo que se les ha enseñado.

Asegurarse de que el material sea relevante

Asegurarse de que el contenido de aprendizaje sea relevante para los usuarios finales es esencial para asegurarse de que sigan participando. Cuando a un usuario final se le presenta información que considera que no es relevante para él, rápidamente comenzará a perder interés y a prestar menos atención.

El material de aprendizaje no solo debe evitar la jerga y los términos técnicos, sino que también debe estar elaborado teniendo en cuenta situaciones de la vida real que el usuario final promedio encontraría en su vida laboral diaria.

Por ejemplo, la mayoría de los empleados no necesitan conocer los detalles de las regulaciones o los ataques de malware, sino simplemente cómo comportarse de una manera que reduzca esos riesgos y cómo informar adecuadamente los riesgos que puedan encontrar.

Financiado por la Unión Europea NextGenerationEU

Ofrecer consejos prácticos

Usar video y contenido interactivo

No todo el contenido es igual. El contenido basado en texto se vuelve aburrido para los usuarios rápidamente y solo debe usarse cuando se complementa con contenido visual más atractivo. Los videos son excelentes para mantener entretenidos a los usuarios, siempre que sean de alta calidad y agradables de ver. El humor se puede utilizar con gran efecto para hacer que los videos de concienciación sobre seguridad sean más atractivos para los usuarios finales.

El contenido interactivo también es excelente para atraer a los usuarios. Muchas personas aprenden haciendo, respondiendo preguntas o participando en su aprendizaje, y el contenido interactivo también puede dar a los usuarios una sensación de logro al completar un curso.

Probar el progreso de los usuarios

Es esencial que después de las sesiones de capacitación, los usuarios sean evaluados sobre lo que han aprendido. Esto te ayuda a saber que los usuarios han aprendido puntos clave y se están alejando después de haber aprendido algo, pero también ayuda al proceso de aprendizaje de los usuarios a medida que recuerdan la información que acaban de aprender de su propia memoria.

Crear una cultura de seguridad

Sin embargo, la parte más esencial de la eficacia de un programa de formación de concienciación sobre la seguridad tiene tanto que ver con factores ajenos a la formación como con la formación misma. Para que la capacitación sea eficaz, debe ser parte de una cultura de seguridad en la que la seguridad siempre recibe la consideración que necesita y se alienta activamente a los usuarios a plantear inquietudes y hacer preguntas.

Un buen programa de concientización sobre seguridad contribuye a esto al presentar la seguridad como algo que es continuo y activo, en lugar de una sola vez y pasivo, pero es esencial que la organización apoye este esfuerzo también fuera de la capacitación.

Cómo integrar la seguridad en la cultura cotidiana del personal

La formación de concienciación sobre seguridad no será eficaz para mejorar los resultados de seguridad si no va acompañada de un cambio cultural. La capacitación integral enseñará a los usuarios finales cómo reconocer situaciones en las que la seguridad está en riesgo y cómo lidiar con ellas de manera adecuada, pero este conocimiento no se pondrá en práctica a menos que el usuario sienta que la seguridad se valora en su cultura.

Con el creciente número de amenazas presentes, así como la creciente complejidad de los servicios comerciales y el acceso a datos y sistemas desde dispositivos móviles, es imposible saber dónde podría aparecer la próxima amenaza o fuga accidental a tu negocio. Esta es la razón por la que la seguridad no debe consistir en garantizar que los usuarios finales elijan contraseñas seguras o sigan otros pasos específicos, sino en capacitarlos para que sean guardianes activos de tu negocio, tus sistemas, dispositivos y datos.

No pienses en la ciberseguridad como un problema de TI

La cultura tiene que ver con los valores. Para que los empleados se preocupen por la seguridad, es necesario destacarla como un valor en toda la empresa. Esto significa garantizar que la seguridad no sea vista como responsabilidad del equipo de seguridad o de TI, sino como una responsabilidad compartida por todos los empleados.

Incorpora la seguridad a los valores de tu empresa

El cambio cultural y los valores de la empresa tienen que venir de arriba. La alta dirección tiene un papel importante que desempeñar a la hora de enfatizar el papel de la seguridad en el negocio, pero es esencial que hagan crecer, en lugar de dictar, la nueva cultura. Esto significa alentar a los empleados a que tomen un papel activo pidiéndoles que planteen inquietudes relacionadas con sus propios roles e incitándoles a que hagan preguntas y se comprometan con los problemas de seguridad.

De esta manera, los usuarios sienten que están involucrados en el proceso de seguridad y comienzan a pensar activamente en las consideraciones de seguridad en sus propios roles. Es posible que un gerente o alguien en TI no esté completamente familiarizado con todos los procesos del flujo de trabajo de un empleado, por lo que es esencial que los propios usuarios comprendan que deben tomar medidas para garantizar la seguridad de los datos y los sistemas.

Incorporar a la alta dirección

La alta dirección también tiene un papel en el establecimiento de prioridades para el negocio. Cualquiera que trabaje para una aerolínea te dirá que la seguridad es siempre, sin excepción, la máxima prioridad. Todo lo demás viene en segundo lugar. Si bien en la mayoría de las otras empresas la seguridad no es un problema de vida o muerte, es importante recordar cuán dañina puede ser una infracción para una empresa.

Si los clientes ya no sienten que pueden confiarle a una organización su información personal o su negocio, podría ser el fin de la empresa. Debe quedar claro para todos los empleados que la seguridad siempre es lo primero, y que siempre es mejor preguntar y asegurarse que lamentar después.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
KIT DIGITAL

Implementar privilegios mínimos

Para un entorno empresarial seguro, un principio arraigado de privilegio mínimo contribuirá en gran medida a proteger los activos, los datos y los sistemas empresariales. Si bien el principio de privilegio mínimo a menudo se considera una medida técnica, que limita a cada usuario solo a los privilegios que requiere para sus funciones específicas, también debe integrarse directamente en la cultura corporativa. Esto significa alentar a los usuarios a informar activamente cuando tengan acceso a más datos o sistemas de los que necesitan, lo que ayuda a limitar las posibilidades de infracciones.

Implementar recordatorios de las mejores prácticas

En términos de medidas físicas, elementos como carteles pueden ser útiles para construir una cultura de seguridad y también contienen recordatorios útiles sobre temas como la seguridad de las contraseñas. Sin embargo, es importante recordar que el simple hecho de pegar un póster en la pared no logrará nada por sí solo, pero deben usarse como inicio para la discusión o servir como complemento al material de capacitación con el que los usuarios ya están comprometidos.

Asegúrate de recompensar a los empleados

Por último, es importante asegurarse de que los empleados sientan que se valoran sus contribuciones a la seguridad. Cuando los empleados hacen preguntas, siempre se les debe dar tiempo y consideración, y debes asegurarte de que comprendan completamente la respuesta y por qué es importante para la seguridad. Cuando los usuarios plantean problemas de seguridad, siempre deben ser recompensados por prestar atención y trabajar para ayudar a mantener la seguridad de la empresa.

Temas esenciales de capacitación en concientización sobre seguridad

No es solo el formato de la capacitación en conciencia de seguridad lo que importa, sino también lo que incluye. La formación debe agotar todos los temas básicos, sin abrumar a los usuarios. Si bien cada organización y cada puesto de trabajo tendrá requisitos diferentes, hay algunas áreas esenciales que vale la pena asegurarse de que todos los usuarios finales las conozcan, aunque sea brevemente.

Estos temas incluyen:

Uso seguro de Internet y correo electrónico

Concienciación sobre el phishing

Seguridad en casa

Contraseñas y autenticación

Trabajando de forma remota

Media removible

Seguridad física

Seguridad de dispositivos móviles

Wi-Fi público

Seguridad en la nube

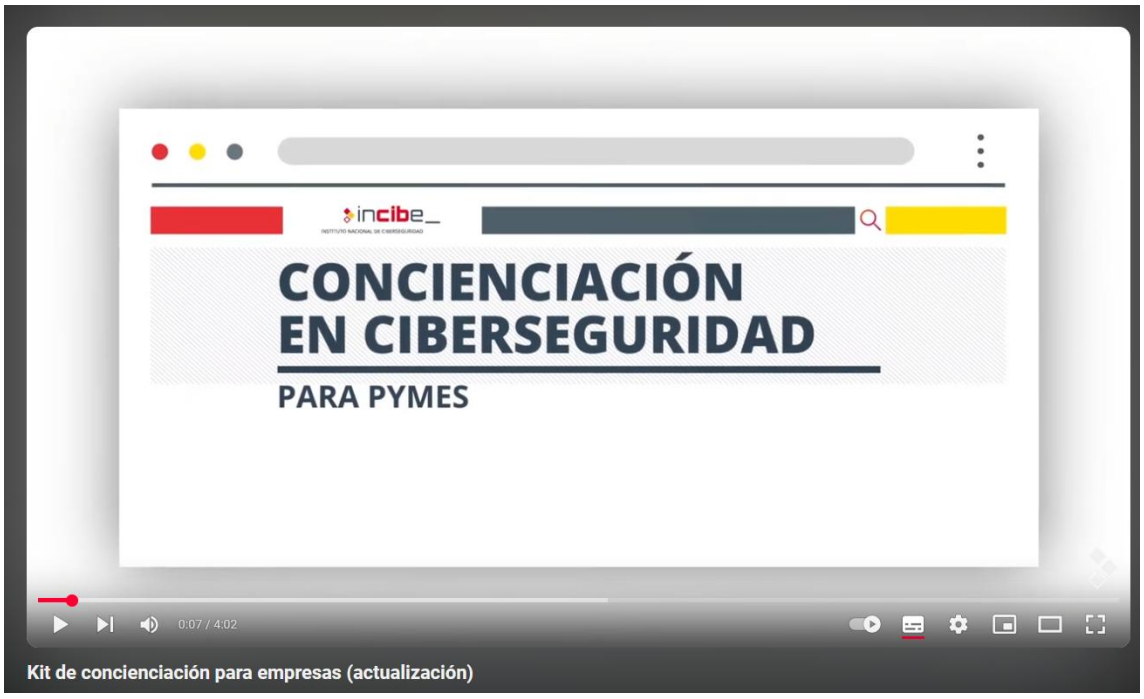
Uso seguro de las redes sociales

Ingeniería social

A medida que evolucionan las nuevas amenazas, continúa probando a tus usuarios finales todos los meses. Haz un seguimiento de los empleados con dificultades y hazles saber cómo se protegen contra el phishing y otras amenazas cibernéticas.

Por último, comparte consejos para la seguridad personal con tus empleados. Comparte consejos sobre wifi público, skimmers de tarjetas de crédito, su contraseña bancaria y más. Cuando los empleados comprenden que la seguridad afecta su vida personal, es mucho más probable que tomen esa información y la apliquen a sus vidas laborales.

Vídeo “Kit de concienciación para empresas”:



https://www.youtube.com/watch?v=AFYZSFWD-Qo

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
KIT DIGITAL

14. Apéndices y Recursos Adicionales

- Sitio oficial de Bitdefender
- Guías de ciberseguridad de Red.es
- https://www.bitdefender.es/consumer/support/guias-de-usuario/
- https://www.bitdefender.com/content/dam/bitdefender/consumers/case-studies/internet-security/ES.pdf
- https://www.bitdefender.com/content/dam/bitdefender/business/products/business-security/es/Bitdefender-GravityZone-Business-Security-Datasheet_es.pdf