Manual de la caja de herramientas de ciberseguridad para pequeñas empresas de la GCA

Bienvenido

Estimado colega:

Internet es una parte integral del negocio de la mayoría de las empresas en estos días. Asegurar el ecosistema digital de su negocio debe ser parte de su forma de trabajar. Un ciberataque puede tener consecuencias devastadoras, incluyendo pérdidas financieras, robo de información sensible, cadenas de suministro comprometidas y más.

Usted tiene muchas otras preocupaciones y responsabilidades, y hemos trabajado para proporcionar un recurso que realmente puede utilizar para abordar sus necesidades de ciberseguridad. La caja de herramientas de ciberseguridad para pequeñas empresas de la Global Cyber Alliance (GCA) proporciona herramientas gratuitas y eficaces para reducir su ciberriesgo. Las herramientas se han seleccionado y organizado cuidadosamente para facilitar la búsqueda e implementación de pasos importantes que ayudarán a defender su negocio contra las ciberamenazas. Hemos incluido vídeos, así como un foro de la comunidad, en los que puede encontrar apoyo y obtener respuestas a preguntas de sus compañeros y expertos en seguridad. La caja de herramientas está diseñada para usted, no para una hipotética pequeña empresa con expertos en ciberseguridad en el personal y un gran presupuesto.

El Manual de la caja de herramientas de ciberseguridad para pequeñas empresas de la GCA es un complemento de la caja de herramientas para ayudar a guiarle en su uso. Puede descargar el manual en su totalidad, o capítulo por capítulo, a medida que avanza a través de las acciones recomendadas en la caja de herramientas. Esta guía facilita su capacidad de trabajar a su propio ritmo para tomar medidas y será un práctico documento de referencia a su conveniencia.

Estos recursos se actualizarán periódicamente con la aportación de usuarios, expertos de la industria y socios de todo el mundo.

¡Esperamos que aproveche la caja de herramientas y el manual para empezar a mejorar su ciberseguridad hoy mismo!

Atentamente,

Philip Reitinger
Presidente y CEO

Índice

Capítulos del manual

Conozca su Sistema

¿Qué problema aborda esta caja de herramientas?

Saber lo que tiene es el primer paso para mejorar la seguridad simplemente porque no puede proteger lo que no sabe que tiene. Tenga en cuenta que muchos ciberataques y vulneraciones de datos son causados por portátiles y otros dispositivos perdidos o robados, acceso no autorizado a cuentas y vulnerabilidades de software sin parches. Al saber qué equipos, dispositivos y software tiene (es decir, sus activos), comprenderá mejor los riesgos potenciales que podrían existir, lo que le permitirá tomar decisiones informadas y tomar medidas para reducir esos riesgos.

- ¿Sabe cuántos portátiles y dispositivos móviles tiene su empresa, quién tiene acceso a ellos y qué software y aplicaciones hay en ellos?
- ¿Sabe qué antigüedad tienen sus equipos y cuándo actualizó por última vez su seguridad?
- ¿Tiene algún sistema o dispositivo conectado a Internet (como cámaras de seguridad o controles de edificios) que también esté conectado a su red empresarial?

Estos activos podrían ofrecer una ruta a su entorno empresarial que un pirata podría utilizar para robar o corromper sus datos. Claramente, saber qué dispositivos y sistemas tiene es importante. Algunos de sus activos son más críticos para las operaciones empresariales que otros, y tener un inventario completo y actualizado le ayuda a priorizar lo que debe protegerse y a qué nivel.

¿Qué le ayudará a lograr esta caja de herramientas?

Después de completar esta caja de herramientas, comprenderá mejor:

- ✔ **cómo llevar a cabo un inventario de sus datos y sistemas**
- ✔ **qué dispositivos y aplicaciones son críticos para las operaciones de su negocio**

Cómo utilizar la caja de herramientas

Utilice las herramientas de la ***caja de herramientas Conozca su sistema*** para ayudarle a identificar todos sus dispositivos (incluidos equipos de sobremesa, portátiles, teléfonos inteligentes e impresoras) y aplicaciones (por ejemplo, correo electrónico, software, exploradores web y sitios web) para que pueda tomar medidas para protegerlos.

Puede emplear este inventario como guía y lista de verificación mientras consulta las demás cajas de herramientas. No se olvide de actualizar el inventario periódicamente y siempre que incorpore o quite un nuevo equipo, cuenta o datos críticos.

Descargue las herramientas del sitio web y anote las fechas completadas. Además, aproveche esta oportunidad para programar una revisión periódica para asegurarse de que toda su información esté actualizada.

Navegar por las subcategorías de la caja de herramientas e información adicional a tener en cuenta

1.1 Identifique sus dispositivos

Al crear un inventario es importante tener en cuenta todo en su entorno.Esto incluye elementos como equipos de escritorio, portátiles, teléfonos inteligentes, impresoras, CCTV, PoS, dispositivos IoT y enrutadores.

Muchos dispositivos IoT de consumo no tienen, o apenas tienen, seguridad integrada, así que considere si puede ser posible separarlos del resto de la red o eliminarlos por completo.

Los equipos más antiguos pueden estar fuera de garantía y ya no están protegidos contra nuevas vulnerabilidades, pero son importantes para las operaciones comerciales. Estos deben identificarse como parte de su inventario y debe desarrollar un plan para reemplazar, actualizar o restringir su uso.

Muchos dispositivos como enrutadores, CCTV e impresoras a veces se olvidan al pensar en el entorno de TI, pero cualquier cosa que tenga una conexión a Internet o a la red local debe tenerse en cuenta al realizar el inventario de los activos porque estas conexiones a menudo proporcionarán una ruta de acceso a su negocio potencialmente fácil.

Identifique dónde se encuentran los datos sensibles y críticos para el negocio, ya sea en dispositivos independientes conectados a la red o en la nube. Puede ser que se deban considerar niveles adicionales de protección para estos dispositivos, pero el primer paso es documentar dónde se guarda todo.

1.2 Identifique sus aplicaciones

Identifique todas sus aplicaciones, incluidas las aplicaciones empresariales, las cuentas en línea para las que utiliza la dirección de correo electrónico de su empresa y otras aplicaciones a las que accede de forma local o remota a través de sus dispositivos.

Es importante tener en cuenta todas las aplicaciones y cuentas, recordando las que ya no utiliza, sobre todo porque es poco probable que esté actualizando el software para ellas. Si no le proporcionan ningún beneficio, elimínelas o cierre las cuentas. Una cuenta en línea antigua puede

contener parte de sus datos personales, y si la organización para la que configuró originalmente esa cuenta ha sufrido una vulneración, sus datos podrían verse afectados.

Encontrará información adicional, soporte y guía durante la implementación a través de la **categoría Conozca su sistema** en el Foro de la comunidad de la GCA.

Enlaces a Conozca su sistema:

Caja de herramientas: ***Caja de herramientas Conozca su sistema***
https://gcatoolkit.org/es/pequenas-empresas/conozca-su-sistema/

Foro de la comunidad: categoría Conozca su sistema
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/know-what-you-have/

El foro en otros idiomas
https://community.globalcyberalliance.org/t/language-support-on-the-forum-de-es-fr-id/

Actualice sus defensas

¿Qué problema aborda esta caja de herramientas?

Los ciberdelincuentes buscan puntos débiles y defectos (conocidos como vulnerabilidades) que se pueden utilizar para obtener acceso a los sistemas o difundir software maligno. Los actores malignos podrían tener acceso a las cuentas financieras de su empresa, a los datos de sus clientes y mucho más. Puede ayudar a protegerse contra esto actualizando sus defensas (es decir, manteniendo sus sistemas, dispositivos y datos actualizados). Los fabricantes y desarrolladores de software publican periódicamente actualizaciones de seguridad para sus sistemas operativos y aplicaciones con el fin de resolver los nuevos puntos débiles o vulnerabilidades que se detectan. Estas correcciones se conocen popularmente como "parches" y su aplicación, como aplicación de parches.

Esta caja de herramientas aborda la necesidad de aplicar estos parches de manera oportuna, incluida la configuración de los sistemas para que se puedan aplicar automáticamente siempre que sea posible. Además, es importante darse cuenta de que, con el tiempo, muchos sistemas se añaden, se adaptan o se reconfiguran, lo que puede conducir a la introducción de puntos débiles que podrían ser explotados por los ciberdelincuentes. Otro problema a tener en cuenta es si un proveedor externo tiene acceso a los datos que hay dentro de sus sistemas. Es importante mantener registros

actualizados; le permite administrar las actualizaciones necesarias para asegurarse de que los parches más actuales se aplican a sus sistemas, dispositivos y aplicaciones.

¿Qué le ayudará a lograr esta caja de herramientas?

Después de completar esta caja de herramientas, comprenderá mejor cómo:

- ✔ comprobar que está ejecutando la última versión del software en su dispositivo
- ✔ configurar sus dispositivos para que acepten y apliquen automáticamente actualizaciones de seguridad
- ✔ implementar ajustes de configuración seguros para dispositivos móviles, exploradores web y sistemas operativos

Cómo utilizar la caja de herramientas

Utilice las herramientas de la ***caja de herramientas Actualice sus defensas*** para asegurarse de que sus dispositivos y aplicaciones está configurados con los parches de seguridad más recientes aplicados y con los niveles de seguridad adecuados para el tipo de datos que contienen. Si ha creado un inventario en la caja de herramientas Conozca su sistema, utilícelo como guía y lista de comprobación para asegurarse de que todos los dispositivos están actualizados y configurados para aceptar automáticamente las actualizaciones de seguridad.

Una vez que haya completado la caja de herramientas Actualice sus defensas, actualice su lista de comprobación de seguridad y establezca un recordatorio para repetir este proceso periódicamente para que se convierta en rutina.

Navegar por las subcategorías de la caja de herramientas e información adicional a tener en cuenta

2.1 Actualice sus dispositivos y aplicaciones

Cuando una solución, o parche, se desarrolla y lanza para una vulnerabilidad conocida, es importante que todos los usuarios de ese sistema o aplicación apliquen estos parches inmediatamente; lo ideal sería de forma automática porque hasta que se hace están en riesgo de compromiso a través de esta vulnerabilidad.

Compruebe cada dispositivo y aplicación y configúrelos para que se actualicen automáticamente. Hemos proporcionado una lista de los sistemas y aplicaciones más comunes, pero para aquellos que

no están cubiertos en esta caja de herramientas, consulte las instrucciones o páginas de soporte para ese dispositivo o aplicación en particular. Tache cada elemento de la lista a medida que avance y no olvide seguir este paso cada vez que incorpore un nuevo dispositivo o aplicación en su compañía.

A menudo, la configuración más segura no se proporciona como la configuración de seguridad predeterminada para sus dispositivos o aplicaciones, ya que la facilidad de uso y la comodidad se priorizan sobre la seguridad. Por lo tanto, debe comprobar si hay alguna configuración de seguridad recomendada por el fabricante para sus dispositivos y aplicaciones e implementarla.

Los dispositivos que ya no son compatibles deben eliminarse, ya que siempre estarán en riesgo de comprometerse con cualquier punto débil recién descubierto. Si esto no es posible, deberían aislarse de otros dispositivos y su uso debería quedar restringido a funciones empresariales específicas solamente.

Las herramientas que se encuentran en esta caja de herramientas ofrecen instrucciones de configuración para que los sistemas comunes apliquen automáticamente las actualizaciones. Debe comprobar la guía de todos sus dispositivos y sistemas para asegurarse de que están configurados en consecuencia.

2.2 Cifre sus datos

Si su red informática sufre una vulneración, hay una alta probabilidad de que el pirata intente robar información sensible o confidencial, que puede utilizar para su propio beneficio financiero o político. Mediante el cifrado de los datos que se almacenan en su disco duro, resulta mucho más difícil para los delincuentes hacer uso de estos datos, ya que tendrá que descifrarlos antes de poder utilizarlos.

El cifrado es el proceso mediante el que los datos se convierten de un formato legible (texto normal) a una formato codificado (texto cifrado). Esta codificación está diseñada para que resulte ininteligible, excepto por las partes que poseen las claves para revertir el proceso de codificación. El cifrado permite almacenar y transmitir datos de forma confidencial y demostrar que la persona que afirma haberlos enviado es quien realmente los creó.

Estas herramientas le permiten cifrar archivos almacenados en su disco duro. Si su sistema operativo no está incluido en la caja de herramientas aquí, es posible que haya más opciones disponibles a través del fabricante del equipo u otras ofertas de seguridad disponibles comercialmente.

2.3 Proteja sus sitios web

Para muchas empresas, su sitio web es fundamental para las operaciones comerciales. Su uso puede incluir el flujo de información sensible a través de la cadena de suministro o puede ser la principal plataforma de negociación en la que se basa su negocio. En caso de que los piratas informáticos obtengan acceso al sitio web que podrían interceptar o robar datos, cambiar su contenido, infectar el

sitio web con malware o hacerse cargo de las operaciones. Cualquiera de estos podría tener un impacto devastador en la capacidad operativa de su organización.

Aquí encontrará herramientas que puede utilizar para ejecutar comprobaciones periódicas en su sitio web (conocidos como análisis) para identificar vulnerabilidades y posibles puntos débiles. Asegúrese de que el personal competente de TI evalúe los problemas identificados y adopte las medidas apropiadas.

Las subcategorías de la caja de herramientas proporcionan instrucciones y herramientas para los sistemas de uso común. Para otros, busque ayuda a través del sitio web del proveedor o pida consejo en el Foro de la comunidad de la GCA: **categoría Actualice sus defensas** o **Comunidad para pequeñas empresas**.

Enlaces a Actualice sus defensas:

Caja de herramientas: ***Caja de herramientas Actualice sus defensas***
https://gcatoolkit.org/es/pequenas-empresas/actualice-sus-defensas/

Foro de la comunidad: **categoría Actualice sus defensas**
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/update-your-defences/

Comunidad para pequeñas empresas
https://community.globalcyberalliance.org/c/community-discussions/small-business-community/

Renuncie a las contraseñas simples

¿Qué problema aborda esta caja de herramientas?

Las contraseñas son una primera línea de defensa para proteger sus cuentas y datos (como correo electrónico, registros de personal o bases de datos de clientes).

Desafortunadamente, las contraseñas suelen ser un blanco fácil para los ciberdelincuentes y las vulneraciones de datos relacionadas con la piratería a menudo ocurren debido a contraseñas débiles. Los atacantes tienen muchas maneras de tratar de acceder a sus contraseñas, desde el uso de crackers de contraseña que pueden obtener fácilmente, que son programas que recorren combinaciones de uso común, hasta el uso de un nombre de usuario y contraseña obtenidos de una cuenta que sufrió una vulneración, y probándolos en otros sitios populares. Estas técnicas necesitan poca capacidad técnica, son rápidas, totalmente automatizadas y están fácilmente disponibles para aquellos que saben dónde buscarlas en Internet. El problema para las pequeñas y medianas empresas es que muchas no tienen una política de contraseñas o, si la tienen, no la aplican estrictamente.

Por lo tanto, tener contraseñas seguras es vital para proteger sus datos. Pero también debe dar otro paso más mediante la implementación de la autenticación de doble factor o multifactor (2FA).

La autenticación de doble factor requiere varias credenciales, lo que hace mucho más difícil para un atacante obtener acceso a sus cuentas.

Con la autenticación de doble factor, un usuario necesita lo siguiente:

- Algo que conoce, como una contraseña;
- Y algo que tiene, como un token (Google Authenticator, Authy, Okta, RSA, etc.) o un código de verificación enviado a su teléfono; o bien
- Algo que es, como su huella digital o su cara (biometría).

Esta caja de herramientas le ayuda a crear contraseñas más fuertes y únicas para cada una de sus cuentas y le muestra cómo configurar la autenticación de doble factor, que son pasos importantes para proteger el acceso a sus cuentas y datos.

¿Qué le ayudará a lograr esta caja de herramientas?

Después de completar esta caja de herramientas, comprenderá mejor cómo:

- ✔ crear una contraseña segura
- ✔ probar sus cuentas para ver si han sido comprometidas
- ✔ configurar la autenticación de doble factor para las cuentas en línea más comunes

Cómo utilizar la caja de herramientas

Utilice las herramientas de la ***caja de herramientas Renuncie a las contraseñas simples*** para asegurarse de que sus dispositivos y aplicaciones están configurados con contraseñas seguras y la autenticación de doble factor. Si ha creado un inventario en Conozca su sistema, utilícelo como guía y lista de comprobación para asegurarse de que lo ha implementado en todas sus cuentas.

Una vez que haya completado la caja de herramientas Renuncie a las contraseñas simples, actualice su lista de comprobación de seguridad y establezca un recordatorio para repetir este proceso periódicamente para que se convierta en rutina.

Navegar por las subcategorías de la caja de herramientas e información adicional a tener en cuenta

3.1 Contraseñas seguras

Uno de los métodos más comunes que emplean los delincuentes para obtener acceso a sus cuentas, su red o su información es iniciar sesión haciéndose pasar por usted. Es muy importante que:

- Use una contraseña única y segura (o frase de contraseña) para cada una de sus cuentas.
- Utilice letras, números y caracteres especiales para garantizar una contraseña segura.
- Cambie su contraseña inmediatamente si ha sufrido una vulneración.
- Mantenga sus contraseñas privadas y seguras.
- Nunca reutilice una contraseña.
- Nunca haga clic en un enlace en un correo electrónico que le indique "es hora de restablecer su contraseña"; siempre debe acceder al sitio web de la cuenta a través del explorador web.
- Evite iniciar sesión en cuentas a través de wifi público.

Si emplea la misma contraseña en diferentes cuentas y un delincuente consigue hacerse con ella, tendrá acceso a todas esas cuentas. Los detalles de nombre de usuario y contraseña pueden ser vendidos en línea por los delincuentes que los han robado en un ciberataque y ser reutilizados hasta que se cambia la contraseña. El rápido avance de la tecnología significa que un portátil moderno barato puede recorrer rápidamente todas las combinaciones para elaborar contraseñas simples cortas.

Debe tener una política de contraseñas que todo el personal y cualquier contratista que tenga acceso a sus sistemas puedan comprender y deban cumplir. Algunos sistemas y aplicaciones pueden permitirle aplicar una contraseña mínima permitida, por lo que vale la pena comprobarlo en la configuración de seguridad.

Puede utilizar las herramientas de Contraseñas seguras para obtener más información sobre las contraseñas y comprobar si su dirección de correo electrónico ha sido robada en una vulneración. Si es así, cambie su contraseña inmediatamente y nunca reutilice las contraseñas.

Recuerde también comprobar la configuración de contraseña en enrutadores, impresoras y otros equipos conectados a la red. Estos se pueden olvidar fácilmente y generalmente se envían con contraseñas predeterminadas simples. Trabaje con el inventario que creó en Conozca su sistema y márquelo sobre la marcha.

3.2 Herramientas para la autenticación de doble factor

La autenticación de doble factor (2FA) proporciona una segunda línea importante de defensa más allá de las contraseñas para proteger las cuentas del acceso no autorizado. Existen diferentes métodos de autenticación que se pueden utilizar para la autenticación de doble factor. Estos van desde un código único enviado a través de texto a su teléfono móvil, un token de hardware que lleva consigo, una huella digital o el reconocimiento facial.

Herramientas para la autenticación de doble factor contiene recursos descargables que proporcionan métodos de autenticación aceptados para muchas cuentas comunes.

Al implementar las herramientas y las instrucciones de la caja de herramientas Renuncie a las contraseñas simples, tenga en cuenta también qué permisos tiene cada usuario al acceder a aplicaciones relacionadas con el negocio. Considere la posibilidad de restringir el acceso solo a aquellos que lo necesitan y en la medida en que su rol lo requiera.

3.3 Administre sus contraseñas

Los administradores de contraseñas son una forma de mantener todas sus contraseñas juntas de forma segura sin necesidad de recordar cada una individualmente. Esto significa que solo necesita recordar una contraseña cada vez que desee iniciar sesión en una de las cuentas cuya contraseña se almacena en el administrador de contraseñas. Los administradores de contraseñas ofrecen más comodidad. Sin embargo, también significa que si el administrador de contraseñas se ha visto comprometido, el atacante tendría acceso a todas las contraseñas.

Encontrará información adicional, soporte y guía durante la implementación a través de la **categoría Renuncie a las contraseñas simples** en el Foro de la comunidad de la GCA.

Enlaces a Renuncie a las contraseñas simples:

Caja de herramientas: ***Caja de herramientas Renuncie a las contraseñas simples***
https://gcatoolkit.org/es/pequenas-empresas/renuncie-a-las-contrasenas-simples/

Foro de la comunidad: categoría Renuncie a las contraseñas simples
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/beyond-simple-passwords/

Protéjase contra el phishing y el malware

¿Qué problema aborda esta caja de herramientas?

Cada año, muchas pequeñas empresas son víctimas de costosos ataques de malware y phishing. Cuando un usuario hace clic en un sitio web infectado con malware o abre un archivo adjunto infectado en un correo electrónico de phishing, el resultado puede ser la eliminación o modificación de archivos, aplicaciones modificadas o funciones del sistema desactivadas.

El malware es cualquier software que está diseñado para causar daños o acceso no autorizado a dispositivos o redes. Los correos electrónicos de phishing engañan al usuario haciéndole creer que están tratando con una entidad de confianza para que el atacante pueda obtener acceso no autorizado a contenido privado, sensible, restringido o económico. El atacante hará todo lo que pueda para que su correo electrónico parezca genuino y atractivo para que el usuario haga clic en él o lo abra. Los correos electrónicos pueden parecer que provienen de alguien que conoce, pueden imitar los logotipos y el formato de los correos electrónicos de organizaciones conocidas o pueden referirse a titulares recientes o a un trabajo que acaba de hacer.

Algunas estimaciones sugieren que más del 90 % de los ciberataques comienzan con un correo electrónico de phishing. Si hace clic en el enlace o abre el archivo adjunto en un correo electrónico de phishing, puede desencadenar una serie de actividades que el atacante ha configurado y entre las que se podrían incluir el robo de sus datos, la creación de una ruta secreta (conocida como puerta trasera) en su equipo para su uso posterior, la instalación de un tipo de malware a través del cual el atacante le bloquea fuera de sus datos y le pide pagar un rescate por volver a acceder (conocido como ransomware) o descargar otro tipo de malware que permite al atacante ver lo que escribe, como contraseñas o números de cuenta (conocido como spyware).

Las consecuencias de los ataques de phishing y malware son graves para las pequeñas empresas. Los efectos pueden incluir pérdida o daño a los datos, pérdida de ingresos si su negocio se cierra durante un ataque, gastos incurridos para reparar/reemplazar equipos, costos para notificar a los clientes una vulneración, junto con la pérdida de reputación y posibles demandas.

La *caja de herramientas Protéjase contra el phishing y el malware* le ayudará a reducir los riesgos al fortalecer su resistencia a los ataques. Se incluyen herramientas para ayudar a evitar que vaya a sitios web infectados, software antivirus para ayudar a evitar que los virus y otro malware entren en sus sistemas y bloqueadores de anuncios para ayudar a prevenir los anuncios en línea que pueden llevar virus.

¿Qué le ayudará a lograr esta caja de herramientas?

Después de completar esta caja de herramientas, comprenderá mejor:

- ✔ **cómo el software antivirus protege sus sistemas y datos**
- ✔ **cómo instalar software antivirus en su sistema**
- ✔ **anuncios digitales y los riesgos que plantean**
- ✔ **cómo instalar un bloqueador de anuncios para bloquear anuncios emergentes, vídeos y otro contenido no deseado**
- ✔ **qué significa DNS y por qué es importante**
- ✔ **cómo funciona la seguridad de DNS y qué tipos de ataques mitiga**
- ✔ **cómo instalar Quad9 en sus dispositivos Android y equipos**

Navegar por las subcategorías de la caja de herramientas e información adicional a tener en cuenta

Las herramientas se han elegido cuidadosamente sobre la base de normas globales reconocidas y no se presentan aquí en ningún orden en particular o prioridad recomendada.

4.1 Antivirus

Es importante utilizar un antivirus en tiempo real porque este comprueba la existencia de virus en tiempo real, ya que están sucediendo, eliminando así los virus antes de que puedan causar daños, y se actualiza a medida que se desarrolla una nueva protección antivirus.

4.2 Bloqueadores de anuncios

Algunos anuncios o mensajes en línea que aparecen mientras navega por un sitio web son útiles; sin embargo, otros pueden contener código maligno y podrían infectar su equipo con malware si hace clic en el anuncio. Un bloqueador de anuncios se puede utilizar para evitar que los anuncios aparezcan en las páginas web, ofreciendo protección adicional durante la navegación.

4.3 Seguridad de DNS

La seguridad de DNS utiliza el sistema de nombres de dominio (que es el equivalente a Internet de una guía telefónica) para traducir el nombre del sitio web basado en texto (nombre de dominio) que un usuario escribe en el explorador en un conjunto único de números (dirección IP), que los equipos entienden.

Muchos atacantes tratan de utilizar nombres de dominio de sitios web similares para engañar a sus víctimas y hacerles pensar que se están conectando a un sitio legítimo. Estos sitios pueden parecerse al nombre real del sitio web, pero una inspección más cercana puede mostrar diferencias.

Así, por ejemplo, la URL legítima del sitio web de una empresa podría tener este aspecto: "www.mygreatwidgets.com", pero el falso podría tener este aspecto: "www.rnygreatwidgets.com".

Los firewalls de DNS, que son un tipo de seguridad de DNS, pueden ayudar a prevenir virus y ataques de phishing porque comprueban si se sabe que la dirección IP del sitio web que se solicita alberga código maligno y, si es así, bloquea el acceso a él. Los usuarios pueden implementar servicios de filtrado de DNS en sus sistemas utilizando las herramientas de esta subcategoría para ayudar a evitar el acceso a sitios web malignos conocidos.

Las subcategorías de la caja de herramientas proporcionan herramientas para sistemas de uso común. Para obtener más ayuda, busque o haga preguntas en el Foro de la comunidad de la GCA: **categoría Protéjase contra el phishing y el malware** o bien en **Comunidad para pequeñas empresas**.

Enlaces a Protéjase contra el phishing y el malware:

Caja de herramientas: ***Caja de herramientas Protéjase contra el phishing y el malware***
https://gcatoolkit.org/es/pequenas-empresas/protejase-contra-el-phishing-y-el-malware/

Foro de la comunidad: **categoría Protéjase contra el phishing y el malware**
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/prevent-phishing-and-viruses/

Comunidad para pequeñas empresas
https://community.globalcyberalliance.org/c/community-discussions/small-business-community/

Copias de seguridad y recuperación

¿Qué problema aborda esta caja de herramientas?

La pérdida o corrupción de datos podría deberse a un ciberataque (como ransomware) o a un error o robo de equipos, error humano, daño accidental, incendio o inundación. Independientemente de la

causa, el impacto de la pérdida de datos o el tiempo de inactividad del equipo puede afectar seriamente a la productividad y la rentabilidad de su negocio.

Una copia de seguridad es una copia de sus datos, almacenada en una ubicación diferente a los datos originales, y puede ayudarle a recuperarse de un ataque o pérdida de datos. Tener copias de seguridad periódicas y sin conexión facilitará una recuperación más rápida de la pérdida o la corrupción de los datos. Ambos son importantes porque las copias de seguridad en línea están configuradas para realizar copias de seguridad automáticamente en una red, mientras que las copias de seguridad sin conexión requieren la conexión y posterior extracción de un dispositivo externo (por ejemplo, un USB o un disco duro) para el almacenamiento físico en otro lugar (lo que también ayuda a protegerse contra la copia de seguridad involuntaria de datos ya dañados).

¿Qué le ayudará a lograr esta caja de herramientas?

Después de completar esta caja de herramientas, comprenderá mejor:

- ✔ **por qué las copias de seguridad son importantes para su negocio, especialmente en la recuperación de un ataque ransomware**
- ✔ **cómo habilitar la copia de seguridad completa en su máquina Windows o Mac**

Cómo utilizar la caja de herramientas

Utilice las herramientas de la ***caja de herramientas Copias de seguridad y recuperación*** para asegurarse de que sus sistemas se copian periódicamente, en un nivel y con una frecuencia adecuados para el tipo de datos que contienen.

¿De qué debería hacer una copia de seguridad? Eso depende de su información y del riesgo de pérdida de dicha información. Si creó un inventario en la caja de herramientas Conozca su sistema, utilícelo como guía y lista de comprobación, y actualícelo a medida que avanza.

Una vez que haya completado la caja de herramientas Copias de seguridad y recuperación, actualice su lista de comprobación de seguridad y establezca un recordatorio para revisarla periódicamente para asegurarse de que su política siga siendo adecuada para su negocio.

Navegar por las subcategorías de la caja de herramientas e información adicional a tener en cuenta

El ransomware es un método de ataque que se ha convertido en un problema grave para las pequeñas empresas. El ransomware es un tipo de software maligno que infecta los equipos y bloquea

el acceso a los datos. El autor exige el pago, a veces en forma de criptomoneda, (es decir, bitcoin, que es menos fácil de rastrear que las transferencias tradicionales), con la promesa de que los datos se restaurarán una vez que se reciba el rescate. Disponer de copias de seguridad de sus datos es una salvaguarda importante para acceder a su información si es víctima de ransomware.

5.1 Copias de seguridad según sistema operativo

Tener una política de copia de seguridad sólida que incluya copias de seguridad tanto en línea como sin conexión ayuda a facilitar una recuperación más rápida de la pérdida o corrupción de datos.

- Los diferentes conjuntos de datos que tiene deben clasificarse en el inventario (consulte la caja de herramientas Conozca su sistema para obtener ayuda sobre cómo crear un inventario).
- Considere el uso de cifrado para la información sensible (consulte la caja de herramientas Actualice sus defensas para obtener más información sobre el cifrado).
- Implemente un enfoque sensato para realizar una copia de seguridad de cada conjunto de datos, teniendo en cuenta el "impacto de la pérdida" de cada uno de ellos. El impacto de la pérdida puede ser de reputación, financiero o legal.

En la subcategoría Copias de seguridad según sistema operativo, encontrará instrucciones sobre las copias de seguridad en sistemas operativos comunes. Si el suyo no está incluido, busque ayuda a través del sitio web de su proveedor o pregunte en la **categoría Copias de seguridad y recuperación** en el Foro de la comunidad de la GCA.

Asegúrese también de que tiene un plan de recuperación ante desastres, que ayuda a habilitar la recuperación de sistemas críticos después de un desastre (ya sea un desastre accidental o natural). Tener un plan ayuda a minimizar el tiempo de recuperación y el daño a los sistemas, protege contra posibles responsabilidades y también puede mejorar la seguridad. Hay muchas plantillas y guías disponibles en línea para desarrollar un plan. Asegúrese de mantenerlo actualizado y realice escenarios simulados para ejercer el plan y asegúrese de que todos sepan cómo implementarlo.

Enlaces a Copias de seguridad y recuperación:

Caja de herramientas: ***Caja de herramientas Copias de seguridad y recuperación***
https://gcatoolkit.org/es/pequenas-empresas/copias-de-seguridad-y-recuperacion/

Foro de la comunidad: **categoría Copias de seguridad y recuperación**
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/back-up-and-recover/

Proteja su correo electrónico y reputación

¿Qué problema aborda esta caja de herramientas?

El correo electrónico se utiliza a menudo como punto de partida para un ciberataque. Resulta extremadamente rápido y barato enviar miles de correos electrónicos a destinatarios desprevenidos con la esperanza de que al menos algunos de ellos caigan en la trampa y hagan clic en el enlace de un sitio web maligno o descarguen un archivo adjunto dañino.

Una de las técnicas que utilizan los ciberdelincuentes es hacer que el correo electrónico aparezca como si se hubiera enviado desde una fuente legítima, como su institución financiera, un cliente, un socio comercial u otra organización familiar. Una de estas técnicas se conoce como spoofing de dominio de correo electrónico, en la que la dirección de correo electrónico "suplantada" utilizada es exactamente la misma que la genuina, por lo que parece haber sido enviada realmente desde esa organización, dando al receptor pocas razones para sospechar que no ha sido enviado realmente desde ellos.

Si el dominio de correo electrónico de su empresa (la parte de su dirección de correo electrónico después de la arroba “@”) es falsificado, esto podría tener graves consecuencias para usted, sus clientes y la cadena de suministro. Si el destinatario del correo electrónico tomó medidas en el correo electrónico porque realmente creía que provenía de usted, esto podría llevar a que su sistema informático se infectara con alguna forma de malware o ransomware. También podría permitir que el criminal tome el control y manipule sus datos bancarios, para que los clientes hagan pagos a otras cuentas pensando que le están pagando a usted.

La caja de herramientas Proteja su correo electrónico y reputación proporciona orientación y herramientas para protegerse contra este tipo de amenazas, incluyendo la guía para el uso de un estándar de correo electrónico conocido como DMARC (Autenticación basada en dominios, informes y conformidad). DMARC es una manera eficaz de evitar que los spammers y phishers utilicen los dominios de la empresa para llevar a cabo ciberataques peligrosos. Este estándar permite verificar que el remitente de un correo electrónico tiene permiso para usar el dominio y enviar correos electrónicos.

Los atacantes también pueden configurar sitios web "parecidos". Por ejemplo, el dominio genuino "BestBusiness.com" puede ser suplantado mediante el registro de "BestBusness.com" o "BestBusiness.net" para engañar a los clientes o usuarios para que los visiten.

Si su correo electrónico o dominios del sitio web son falsificados, podría resultar en un daño a su reputación y a su marca, así como en un daño a sus clientes. El uso de las herramientas de Proteja su correo electrónico y reputación ayuda a identificar y prevenir la suplantación.

¿Qué le ayudará a lograr esta caja de herramientas?

Después de completar esta caja de herramientas, comprenderá mejor:

- ✔ lo que DMARC significa, por qué es importante y qué ataques mitiga
- ✔ la Guía de configuración de DMARC
- ✔ cómo comprobar su propio dominio de correo electrónico para ver si DMARC está habilitado

Cómo utilizar la caja de herramientas

Utilice las herramientas de la ***caja de herramientas Proteja su correo electrónico y reputación*** para asegurarse de que su empresa está protegida contra la suplantación de dominios de correo electrónico mediante la implementación de DMARC e identificar posibles dominios de sitios web similares.

Actualice su lista de comprobación de seguridad una vez completada y anime a sus clientes y a la cadena de suministro que utilizan su propio dominio a hacer lo mismo, ya que la eficacia de DMARC depende tanto de que el remitente como el receptor hayan implementado DMARC.

Navegar por las subcategorías de la caja de herramientas e información adicional a tener en cuenta

6.1 Implemente DMARC

Utilice las herramientas de esta subcategoría para obtener más información sobre DMARC, compruebe si su dominio de correo electrónico está protegido por DMARC y, si es así, a qué nivel.

6.2 Análisis de informes DMARC

Una vez que se haya configurado una regla de DMARC en su dominio de correo electrónico, empezará a recibir informes que muestran cómo se usa su dominio de correo electrónico. Estos pueden ser difíciles de interrumpir sin formato.

Las herramientas de la subcategoría Análisis de informes DMARC ayudan a proporcionar interpretación e identificación más rápida de la actividad fraudulenta. Esto le permite moverse con confianza a través de los niveles de política de "ninguno" a "cuarentena" y, en última instancia, hasta el nivel más alto de "rechazo". También es importante considerar cualquier organización o servicio de correo electrónico autorizados para enviar correos electrónicos en su nombre, como servicios de marketing por correo electrónico, y comprobar si tienen DMARC implementado.

Solo cuando su dominio de correo electrónico esté en "rechazar" se obtendrá todo el beneficio de DMARC.

6.3 Proteja sus marcas comerciales

Los estafadores pueden registrar dominios que se parecen mucho a su propio dominio con la esperanza de que las personas hagan clic en ellos. Utilice estas herramientas para ayudar a identificar dominios que intentan imitar el suyo, así como dominios que contienen phishing o contenido maligno dirigido a su dominio.

Para obtener más soporte al implementar DMARC, consulte el **Foro de DMARC** o bien la **categoría Proteja su correo electrónico y reputación** en el Foro de la comunidad de la GCA.

Enlaces a Proteja su correo electrónico y reputación:

Caja de herramientas: ***Caja de herramientas Proteja su correo electrónico y reputación***
https://gcatoolkit.org/es/pequenas-empresas/proteja-su-correo-electronico-y-reputacion/

Foro de la comunidad: **Foro de DMARC**
https://community.globalcyberalliance.org/c/dmarc/

Categoría Proteja su correo electrónico y reputación
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/protect-your-email-and-reputation

Glosario

Un glosario de algunos términos de uso común relacionados con la ciberseguridad. Algunos de estos términos se han incluido en los capítulos del Manual de la caja de herramientas de ciberseguridad para pequeñas empresas de la GCA, mientras que otros se proporcionan para obtener información adicional si desea explorar más por su cuenta.

cuenta Generalmente se refiere al acceso a un sistema informático o servicio en línea, por lo general requiere una contraseña para entrar.

adversario Individuo, grupo, organización o gobierno que realiza o tiene la intención de realizar actividades perjudiciales.

antivirus Software que está diseñado para detectar, detener y eliminar virus y otros tipos de software maligno.

aplicación (app) Programa diseñado para realizar tareas específicas. La aplicación a menudo se refiere a los programas descargados en dispositivos móviles.

activo Persona, estructura, instalación, información y registros, sistemas y recursos de tecnología de la información, material, proceso, relaciones o reputación que tenga valor. Cualquier cosa útil que contribuya al éxito de algo, como una misión organizativa; los activos son elementos de valor o propiedades a las que se puede asignar valor.

ataque Intento de obtener acceso no autorizado a los servicios, recursos o información del sistema, o un intento de comprometer la integridad del sistema. El acto intencional de intentar eludir uno o más servicios o controles de seguridad de un sistema de información.

firma de ataque Característica o patrón distintivo que se puede buscar o que se puede utilizar para que coincida con ataques previamente identificados.

superficie de ataque Conjunto de formas en que un adversario puede entrar en un sistema y potencialmente causar daño. Características de un sistema de información que permiten a un adversario sondear, atacar o mantener la presencia en el sistema de información.

atacante Actor maligno que busca explotar los sistemas informáticos con la intención de cambiar, destruir, robar o deshabilitar su información, y luego explotar el resultado.

autenticación Proceso para verificar que alguien es quien dice ser cuando intenta acceder a un equipo o servicio en línea. También el origen y la integridad de los datos, usuario, proceso o dispositivo.

puerta trasera Forma encubierta para que los ciberdelincuentes obtengan acceso no autorizado a un sistema informático

copia de seguridad Copia de sus datos, almacenada en una ubicación diferente a los datos originales que puede ayudarle a recuperarse de un ataque o pérdida de datos.

realizar copia de seguridad Permite hacer una copia de los datos almacenados en un equipo o servidor para disminuir el impacto potencial de un error o pérdida.

bot Equipo o dispositivo conectado a Internet que se ha visto comprometido en secreto con código maligno para realizar actividades bajo el mando y el control de un administrador remoto.

botnet Red de dispositivos infectados (bots), conectados a Internet, utilizados para cometer ciberataques coordinados sin el conocimiento de su propietario.

vulneración Incidente en el que se accede a datos, sistemas informáticos o redes, o estos se ven afectados de forma no autorizada.

ataque por fuerza bruta Usando una potencia de cálculo para introducir automáticamente un gran número de combinaciones de valores, por lo general con el fin de descubrir contraseñas y obtener acceso.

bug Defecto inesperado y relativamente pequeño, error, defecto o imperfección en un sistema de información o dispositivo.

configuración Disposición de los componentes de software y hardware de un sistema informático o dispositivo.

configuración Proceso de definición de los ajustes de software o dispositivos para un equipo, sistema o tarea específicos

ciberataque Intentos malignos de dañar, interrumpir u obtener acceso no autorizado a sistemas informáticos, redes o dispositivos, a través de medios cibernéticos.

incidente cibernético Vulneración de las normas de seguridad de un sistema o servicio; más comúnmente, intentos de obtener acceso no autorizado a un sistema o a datos, uso no autorizado de sistemas para el procesamiento o almacenamiento de datos, cambios en un software o hardware de firmware de sistemas sin el consentimiento de los propietarios del sistema, interrupción maligna o denegación de servicio.

ciberseguridad Protección de los dispositivos, servicios y redes (y la información sobre ellos) contra robos o daños.

criptomoneda Dinero digital. La criptomoneda se almacena en una cartera digital (en línea, en su equipo o en otro hardware). La criptomoneda normalmente no está respaldada por ningún gobierno, por lo que no tiene las mismas protecciones que el dinero almacenado en un banco.

ataque por diccionario Tipo de *ataque por fuerza bruta* en el que el atacante utiliza palabras conocidas del diccionario, frases o contraseñas comunes como sus suposiciones.

huella digital "Huella" de información digital que la actividad en línea de un usuario deja atrás.

denegación de servicio (DoS) Ataque en el que se deniega a los usuarios legítimos el acceso a servicios informáticos (o recursos), normalmente sobrecargando el servicio con solicitudes.

dispositivo Pieza de hardware de equipo diseñada para una función específica, por ejemplo, portátil, teléfono móvil o impresora.

DMARC Son las siglas en inglés de "Autenticación de mensajes basada en dominios, informes y conformidad". DMARC es un mecanismo que permite a los remitentes y receptores monitorizar y mejorar la protección de sus dominio contra correos fraudulentos.

spoofing de dominios de correos electrónicos Técnica utilizada por los ciberdelincuentes en la que la dirección de correo electrónico "suplantada" utilizada es exactamente la misma que la genuina, por lo que parece haber sido enviada realmente desde esa organización.

cifrado Convertir datos en un formato que no pueda ser fácilmente entendido por personas no autorizadas.

firewall Dispositivo de hardware/software o un programa de software que limita el tráfico de red de acuerdo con un conjunto de reglas de qué acceso está permitido o no está permitido o autorizado.

pirata Alguien que vulnera la seguridad informática por razones malignas, elogios o beneficio personal

hardware Equipo, sus componentes y su equipo relacionado. El hardware incluye unidades de disco, circuitos integrados, pantallas de visualización, cables, módems, altavoces e impresoras.

amenaza interna Persona o grupo de personas con acceso o conocimiento interno de una compañía, organización o empresa que podría suponer un riesgo potencial al vulnerar las políticas de seguridad con la intención de causar daño.

Internet de las cosas (IoT) Se refiere a la capacidad de los objetos cotidianos (en lugar de los equipos y dispositivos) para conectarse a Internet. Algunos ejemplos son hervidores de agua, neveras y televisores.

intrusión Acto no autorizado de eludir los mecanismos de seguridad de una red o sistema de información.

sistema de detección de intrusiones (IDS) Programa o dispositivo utilizado para detectar que un atacante ha intentado acceder sin autorización a los recursos informáticos.

sistema de prevención de intrusiones (IPS) Sistema de detección de intrusiones que también bloquea el acceso no autorizado cuando se detecta.

registrador de pulsaciones de teclas Software o hardware que rastrea las pulsaciones de teclas y eventos del teclado, generalmente en secreto, para monitorizar las acciones del usuario de un sistema de información.

publicidad maligna Uso de la publicidad en línea como método de entrega de malware.

malware (software maligno) Término que incluye virus, troyanos, gusanos o cualquier código o contenido que podría tener un impacto adverso en organizaciones o individuos. Software destinado para infiltrarse y dañar o deshabilitar equipos.

mitigación Aplicación de una o más medidas para reducir la probabilidad de que ocurra una ocurrencia no deseada o disminuir sus consecuencias.

red Dos o más equipos vinculados para compartir recursos.

amenaza externa Persona o grupo de personas externas a una organización que no están autorizadas a acceder a sus activos y que representan un riesgo potencial para la organización y sus activos.

contraseña Cadena de caracteres (letras, números y otros símbolos) utilizada para autenticar una identidad o para verificar la autorización de acceso.

crackers de contraseña Programas diseñados para adivinar una contraseña, a menudo mediante un ciclo de combinaciones de uso común o utilizando un nombre de usuario y contraseña obtenidos de una cuenta que sufrió una vulneración.

administradores de contraseñas Programas que permiten a los usuarios generar, almacenar y administrar contraseñas en una ubicación segura.

aplicación de parches Aplicar actualizaciones al firmware o al software para mejorar la seguridad o la funcionalidad.

pentest (pruebas de penetración) Prueba autorizada de una red o sistema informático diseñada para buscar los puntos débiles de seguridad para que se puedan reparar.

información de identificación personal (PII) Información que permite inferir directa o indirectamente la identidad de un individuo.

pharming Ataque a la infraestructura de la red que resulta en que un usuario sea redirigido a un sitio web ilegítimo a pesar de que este haya introducido la dirección correcta.

phishing Correos electrónicos masivos no dirigidos, enviados a muchas personas pidiendo información sensible (como detalles bancarios) o animándoles a visitar un sitio web falso. Forma digital de ingeniería social para engañar a las personas para que proporcionen información sensible.

texto sin formato Información sin cifrar.

servidor proxy Servidor que actúa como intermediario entre usuarios y otros servidores, validando las solicitudes de usuario.

ransomware Software maligno que hace inutilizables los datos o sistemas hasta que la víctima realiza un pago.

recuperación Actividades posteriores a un incidente o evento para restablecer los servicios y operaciones esenciales a corto y medio plazo y restablecer plenamente todas las capacidades a largo plazo.

resiliencia Capacidad de adaptarse a las condiciones cambiantes y de prepararse, soportar y recuperarse rápidamente de las interrupciones.

restaurar Recuperación de datos después de un error o pérdida del equipo

evaluación del riesgo Proceso de identificación, análisis y evaluación del riesgo, junto con las posibles consecuencias perjudiciales, con el fin de notificar las prioridades, desarrollar o comparar cursos de acción e informar de la toma de decisiones.

información de seguridad y gestión de eventos (SIEM) Proceso en el que la información de red se agrega, ordena y correlaciona para detectar actividades sospechosas.

smishing Phishing vía SMS - mensajes de texto masivos enviados a los usuarios pidiendo información sensible (por ejemplo, datos bancarios) o animándoles a visitar un sitio web falso.

firma Patrón reconocible y distintivo. Los tipos de firmas incluirían: firma de ataque, firma digital, firma electrónica.

ingeniería social Manipular a las personas para que lleven a cabo acciones específicas o divulguen información que sea de utilidad para un atacante.

software Se refiere a programas para dirigir el funcionamiento de un equipo o procesar datos electrónicos.

spam Abuso de los sistemas de mensajería electrónica para enviar indiscriminadamente mensajes masivos no solicitados.

spear-phishing Forma más específica de phishing, en la que el correo electrónico está diseñado para que parezca que es de una persona que el destinatario conoce o en la que confía.

spoofing Falsificar la dirección de envío de una transmisión para obtener una entrada ilegal [no autorizada] en un sistema seguro. La suplantación de identidad, el enmascaramiento, el piggybacking y la imitación son formas de spoofing.

spyware Malware que pasa información sobre las actividades de un usuario de equipo a una parte externa.

cadena de suministro Sistema de organizaciones, personas, actividades, información y recursos, para crear y mover productos, incluidos los componentes de productos o servicios de proveedores hasta sus clientes.

sistema Generalmente se refiere a un sistema de uno o más equipos o dispositivos que introducen, generan, procesan y almacenan datos e información.

administrador del sistema (admin) Persona que instala, configura, soluciona problemas y mantiene configuraciones de servidor (hardware y software) para garantizar su confidencialidad, integridad y disponibilidad; también administra cuentas, firewalls y parches; responsables del control de acceso, contraseñas, creación y administración de cuentas.

amenaza Algo que podría causar daño a un sistema u organización.

actor de amenaza Individuo, grupo, organización o gobierno que realiza o tiene la intención de realizar actividades perjudiciales.

troyano (caballo de Troya) Programa informático que se disfraza como software legítimo, pero con una función oculta que se utiliza para piratear el equipo de la víctima. Tipo de malware.

autenticación de doble factor (doble factor) Uso de dos componentes diferentes para verificar la identidad reclamada por un usuario. También conocido como autenticación multifactor.

red privada virtual (VPN) Red cifrada que se suele crear para permitir conexiones seguras para usuarios remotos, por ejemplo en una organización con oficinas en varias ubicaciones.

virus Programa informático que puede replicarse a sí mismo, infectar un equipo sin permiso o conocimiento del usuario, y luego propagarse o propagarse a otro equipo. Tipo de malware

vulnerabilidad Punto débil, o defecto, en el software, un sistema o proceso. Un atacante puede tratar de explotar una vulnerabilidad para obtener acceso no autorizado a un sistema.

whaling Ataques de phishing altamente dirigidos (haciéndose pasar por correos electrónicos legítimos) dirigidos a altos ejecutivos.

gusano Programa autoreplicante, autopropagador e independiente que utiliza mecanismos de red para propagarse. Tipo de malware

Definiciones compiladas a partir de recursos producidos por:

British Standards Institute
https://www.bsigroup.com/en-GB/Cyber-Security/Glossary-of-cyber-security-terms/

National Cyber Security Centre (NCSC-UK)
https://www.ncsc.gov.uk/information/ncsc-glossary

National Initiative for Cybersecurity Careers and Studies (NICCS -US)
https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary

Recursos adicionales:

Glosario del Australian Cyber Security Centre
https://www.cyber.gov.au/acsc/view-all-content/glossary

Global Knowledge
https://www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/

Glosario de términos sobre seguridad del Instituto SANS
https://www.sans.org/security-resources/glossary-of-terms/