12 Formas de protegerte
Recomendaciones
Días de Ciberseguridad

Los 12 días de ciberseguridad, es una actividad de acciones priorizadas de protección de la información que realizamos los últimos 12 días de un año en el instituto de ciberseguridad, tomando como referencia marcos (NIST) y estándares internacionales (Familia ISO 27000) en seguridad de la información, dando como resultado un documento de mejores prácticas de seguridad aceptadas a nivel mundial.

Estos 12 consejos son la realización de una serie de controles que, al aplicarlos en la organización, podemos prevenir, detectar y responder a los ataques más comunes contra sistemas y redes.

Estos controles son dinámicos, y cambian de prioridad año con año, con base en las amenazas actuales o en tendencia y los requerimientos de seguridad identificados en las prestaciones de servicios con nuestros clientes y con base en nuestra experiencia, esto nos permite realizar este documento para implementar un plan de seguridad de madurez media, que pueda permitirnos implementar las bases de un Sistema de gestión de seguridad de la información.

Nuestro documento de 12 días de ciberseguridad, toma un enfoque proactivo en procesos, que nos permite protegerte de cualquier tipo de amenazas sin importar su origen (Naturales, internas a la organización, externas, etc).

¿Qué nos llevó a crear este documento?

Con anterioridad hemos recibido múltiples preguntas ¿Cómo debe una empresa dar el primer paso para implementar un plan de ciberseguridad? ¿Existe un checklist de seguridad que podamos seguir para implementar seguridad? ¿Qué solución antimalware es mejor para prevenir el Ransomware?

Este tipo de preguntas que resultaban muy comunes, nos impulsaron a desarrollar este contenido, que sintetiza múltiple información existente en internet y te ayudará a emprender de forma más objetiva y concisa la implementación de seguridad dentro de tu organización.

¿Cómo implementar los consejos?

No todos los controles son aplicables para todas las empresas, sin embargo, nos ayudarán a dar una comprensión de que es fundamental para proteger tu negocio, datos, sistemas, redes e infraestructuras, y las acciones que debes considerar que podrían afectar tu capacidad para tener éxito en el negocio u operación.

Aún siendo una cantidad pequeña de controles, estos no se pueden realizar o desplegar de forma inmediata, ya que unos te llevarán más o menos tiempo dependiendo de la cantidad de recursos de personal e inclusive económicas, ya que en algunas ocasiones necesitarás desarrollar un plan de evaluación, implementación y gestión de procesos.

Inventario y control de activos de hardware y software

Día 1

“Lo que no se define no se puede medir. Lo que no se mide, no se puede mejorar. Lo que no se mejora, se degrada siempre”. William Thomson Kelvin

Como parte fundamental en la seguridad es importante administrar de forma efectiva (inventariar, rastrear y corregir) todos los activos de hardware y software, esto es importante para hacer que sólo el software autorizado esté instalado y pueda ejecutarse, y que todo el software no autorizado y no administrado se encuentre y se impida su instalación o ejecución, así como para que sólo los dispositivos de red autorizados tengan acceso y los dispositivos no autorizados y no administrados se encuentren y se restrinja el acceso.

¿Por qué es importante el inventario de activos?

El control administrado de todos los dispositivos y hardware en la red juega un papel fundamental en la planificación y ejecución de la generación de las estrategias de prevención, respuesta y continuidad de las operaciones del negocio.

Es necesario contar con una comprensión de los dispositivos que se encuentran conectados a su entorno d

e red y el software que ejecutan los mismos. Esto le generará beneficios a su organización, ya que se vuelve más fácil administrar su red y tenemos una visión más específica sobre qué dispositivos debemos proteger.

¿Cómo podemos desarrollar esto?

Qualys asset inventory: Es una versión gratuita de qualys que permite la generación de inventariado de software y componentes de hardware de equipos, es a través de una consola gestionada por un agente instalable en el equipo(s) (https://www.qualys.com/apps/asset-inventory/)

SysAid: Es un software que nos permite tener un inventario de aplicaciones y software en servidores de estaciones de trabajo y dispositivos de red (https://www.sysaid.com/)

Anipe-IT: Es un software que nos permite tener un inventario de aplicaciones y software (https://snipeitapp.com)

¿Qué debemos de obtener de esto?

Se debe obtener un listado de todos los equipos de red, servidores, pc, dispositivos móviles con el detalle de su número de serie, fabricante, garantía, proveedores, factura, también se deben de incluir un listado de los softwares instalados para prevenir que software no permitido sea utilizado en la organización.

Referencia de control:

- **ISO/IEC 27001:2013** - A.8.1.1, A.8.1.2 – Gestión de activos
- **NIST** - ID.AM-1 e ID.AM-2

Hardening de hardware y software en estaciones de trabajo y servidores

Día 2

El malware y los cibercriminales aprovechan las configuraciones inseguras o las vulnerabilidades en las aplicaciones que se ejecutan en el sistema. Para proteger su empresa, debe asegurarse de que su sistema operativo y sus aplicaciones (especialmente los navegadores web) estén actualizados y configurados de forma segura. Además, debe identificar y aprovechar las funciones de seguridad y antimalware que pueden estar integradas en su sistema operativo para ayudar a proteger su entorno.

¿Por qué es importante el hardening de equipos?

Los dispositivos electrónicos suelen tener configuraciones por defecto ya que los fabricantes velan por la facilidad de despliegue y su uso antes que en la misma seguridad. Cabe resaltar que, a pesar de esto, los fabricantes en la actualidad han comenzado a realizar ciertas modificaciones al respecto, existen algunos que nos brindan manuales o documentos en el que nos explican los controles básicos de seguridad, servicios y puertos abiertos con los que cuentan esos dispositivos, las cuentas o contraseñas por defecto, inclusive el software preinstalado que puede ser explotado al ser vulnerable en un estado por defecto de fábrica.

De forma sincera, es complicado generar combinaciones de cada uno de estos puntos respecto a los potenciales fallos que pueden existir, por ello siempre se debe gestionar de forma continua todos los cambios en las configuraciones para evitar potencial degradación en los mismos, y evitar nuevas vulnerabilidades de seguridad

¿Cómo podemos desarrollar esto?

Puedes utilizar analizadores de vulnerabilidades, aunque dependerá del ambiente en el que se encuentre alojado el activo a analizar, hay ambientes virtualizados, en la nube, de red, etc, dentro de múltiples herramientas podemos encontrar:

OpenVAS – Esta es una herramienta de open source que puedes descargar desde el siguiente enlace: https://openvas.org/
Microsoft Baseline Security Analyzer – es una herramienta de seguridad de Microsoft que nos permite desarrollar una línea base de seguridad, enlace de descarga: https://www.microsoft.com/en-us/download/details.aspx?id=19892
GFI Lan Guard – es una herramienta de seguridad que te permite comprobar los ordenadores donde comprobará todas las contraseñas, los puertos abiertos, las entradas de registro e incluso las conexiones de red inalámbricas: https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard

¿Qué debemos de obtener de esto?

Una lista de servicios y puertos abiertos con los que cuentan esos dispositivos, las cuentas o contraseñas por defecto, para monitorearlas y, en caso de contener una vulnerabilidad, poder parchearla considerando tu evaluación de riesgos.

Referencia de control

- **ISO/IEC 27001:2013 -** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
- **NIST -** PR.DS-6, PR.IP-1

Uso controlado de privilegios administrativos

Día 3

Parte de las principales problemáticas de seguridad en las organizaciones son la mala gestión de cuentas de acceso, así como los privilegios que estas credenciales tienen.

Por ello es importante conocer y gestionar los procesos y herramientas utilizados para rastrear, controlar, prevenir y corregir el uso, la asignación y la configuración de privilegios administrativos en computadoras, redes y aplicaciones.

¿Por qué es importante el control de cuentas privilegiadas?

Los privilegios mal administrados son uno de los métodos principales que las amenazas aprovechan para comprometer la red de las organizaciones. Una de las técnicas que los atacantes utilizan es la mala gestión de privilegios, imagina a un usuario que tiene una estación de trabajo que realiza sus actividades con privilegios de administración, gracias a una mala gestión de cuentas, así como una mala capacitación para los usuarios, un usuario puede ser engañado, y abrir un archivo adjunto de un correo electrónico que es malicioso, o descargar y abrir un archivo de un sitio web malicioso y comprometer la red de la empresa con algún ejecutando el contenido del atacante. Si la cuenta del usuario de la víctima tiene privilegios administrativos, se pueden instalar keyloggers, sniffers o secuestrar la información de la red de la empresa.

¿Cómo podemos desarrollar esto?

Si no contamos con un directorio activo o un sistema que nos permita gestionar las cuentas de los usuarios, será importante realizar en primera instancia un inventariado de los activos informáticos que tenemos en nuestra organización, mismo que puedes recurrir al contenido del día 1 para realizarlo, una vez inventariados los activos de tu organización, será importante acceder a los dispositivos, realizar una enumeración de usuarios en los dispositivos, validar los permisos con los que cuenta y retirar los permisos de administración a quienes no los necesiten.

¿Qué debemos de obtener de esto?

Una lista de cuentas que son utilizadas en los dispositivos en conjunto con sus respectivos accesos para eliminar las cuentas con credenciales excesivas.

Referencia de control

- **ISO/IEC 27001:2013 -** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4
- **NIST -** PR.AC-4, PR.AC-1

Conexión remota y Teletrabajo

Día 4

El teletrabajo se refiere a todas las formas de trabajo fuera de la oficina, incluyendo entornos de trabajo no tradicionales tales como aquellos denominados "trabajo a distancia", "lugar de trabajo flexible", "trabajo en remoto" y "entornos virtuales de trabajo".

Los dispositivos móviles, en general, comparten funciones comunes con los dispositivos de uso fijo como, por ejemplo, redes compartidas, acceso a Internet, correo electrónico y gestión de archivos. Los controles de seguridad de la información para los dispositivos móviles consisten, en general, en aquellos adoptados para los dispositivos de uso fijo y aquellos que hacen frente a las amenazas planteadas por su uso fuera de los locales de la organización.

Es importante implementar y generar políticas e implementar medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en lugares de teletrabajo.

¿Cómo podemos desarrollar esto?

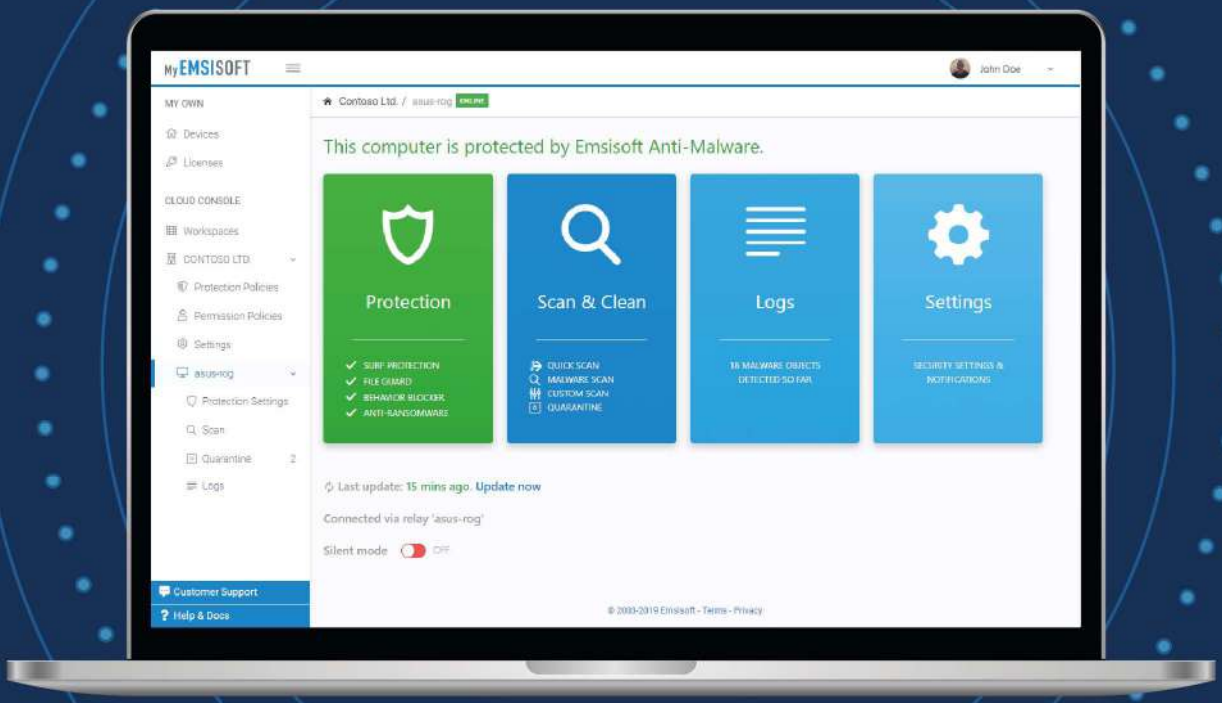
La seguridad en ambientes de teletrabajo se remonta a diversos temas:

Conexión: Lo peor, **lo peor que puedes hacer** es usar Teamviewer, anydesk, o alguna solución de conexión remota de terceros, ojo, **no estamos diciendo que sean malas**, al hacer uso de estos software de control remoto **no podemos gestionar de forma correcta los recursos remotos a los que accede el usuario**, y estos recursos deberían estar asignados basados en las políticas de roles y funciones, nuestra recomendación es **hacer uso de una VPN a través de un Firewall o de un Router** que te permita generar la conexión, el hacer uso de una VPN te permitirá monitorizar el tráfico, así como tener una visión clara de las actividades de tus usuarios y delimitar el acceso a los recursos que el usuario tendrá en tu red, así mismo **te permitirá inhabilitar, eliminar o bloquear conexiones si detectas algo extraño**.

Terminales de servicios críticos: si usas soluciones que funcionan a través de servicios de terminales remotas, es mejor que las uses, sin embargo, no olvides **delimitar el acceso sólo a los recursos que el usuario tenga permitido**.

Escritorios remotos: si los usuarios deben trabajar con recursos internos y te preocupa mucho la seguridad, puedes habilitar un escritorio remoto permitiendo u obligando a trabajar desde el equipo que se encuentra dentro de la red de la empresa (mediante el escritorio remoto), esto te permitirá reducir la posibilidad de ser víctima de robo de datos o será más fácil identificarlo, infectarte con malware será un poco más complicado y te evitará posibles problemas legales. En nuestros despliegues de conexiones remotas con nuestros clientes, nos ha funcionado, más el segundo punto, en especial cuando están trabajando con los equipos personales de los usuarios.

Anti-malware gestionado



Día 5

Las estaciones de trabajo son el motor principal para desempeñar las actividades de los usuarios en tu organización, aquí es donde se almacenan, comparten, modifican datos o información, que en algunas ocasiones serán sensibles o críticas para la operación o continuidad de tu organización, es por eso que debemos protegerlas.

Nuestras estaciones de trabajo suelen estar expuestas a diversas amenazas, principalmente a infecciones por Malware u hoy en día, por secuestro de información que, si sucede, la operación de tu organización se verá completamente afectada.

¿Cómo podemos desarrollar esto?

Implementar soluciones de seguridad antimalware, es importante que estas soluciones de seguridad que vamos a implementar cuenten con algunas de las siguientes características:

- Motor de detección de amenazas basado en comportamiento (es decir que no depende de las firmas de malware, sino que, analiza el comportamiento de cada programa activo en búsqueda de procesos sospechosos)
- Escaneo de archivos de correo electrónico
- Gestión basada en la nube (especificación para administradores de TI)
- Uso de consola en la nube para gestión de estaciones de trabajo.

¿Qué herramientas podemos utilizar?

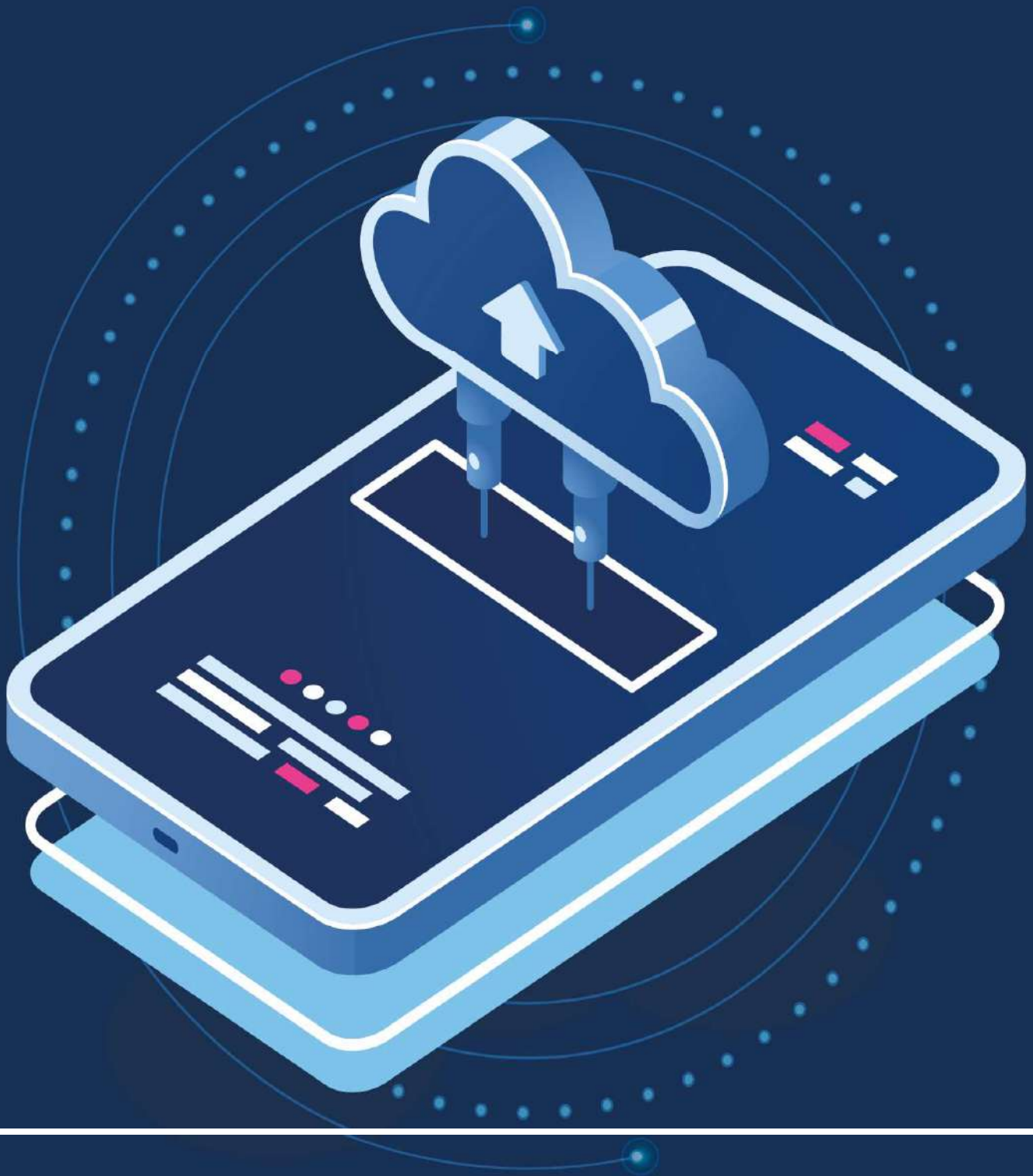
EMSISOFT

Esta herramienta es una solución de prevención antimalware que hemos probado y recomendamos ampliamente (y puedes conseguirla con nosotros), su despliegue o instalación es super fácil de implementar para cualquier tipo de organización, además tiene un enfoque y gran experiencia en el tratamiento, prevención, detección y recuperación de incidentes contra Ransomware, su consola en la nube permite dar una correcta gestión, así como la administración y monitoreo de las estaciones de trabajo, convirtiéndola en una magnifica herramienta de prevención. Puedes probarlo en el siguiente enlace: **https://www.emsisoft.com/en/,** así mismo, puedes adquirir la solución con nosotros, te apoyamos en el dimensionamiento, despliegue y gestión de tu seguridad.

Referencia de control

- **ISO/IEC 27001:2013 -** A.12.2.1
- **NIST -** DE.CM-4

Copias de seguridad



Día 6

A menos que no seas de los que **piensa pagar un laboratorio para que le puedan recuperar su información** después de que esta se ha perdido, entonces este punto te interesa.

Las copias de seguridad son lo que te **permitirá poder recuperarte de un incidente** que dañe, modifique o elimine los activos de información, es por eso que te recomendamos **hacer uso de la regla 3R del instituto de ciberseguridad** para gestión de respaldos:

Respaldar: No importa la solución que uses, sólo haz tu copia de seguridad, puede ser en un USB (Si la información es poca, claro), un equipo NAS o lo que tengas al momento.

Primero identifica tus activos críticos de operación, pueden ser archivos, información e inclusive dispositivos, al identificarlos haz copia de seguridad de ellos, te invitamos a utilizar herramientas especializadas que te permitan gestionar de forma centralizada tus copias, desde la realización automática de la copia (jamás confíen en los usuarios para hacer sus copias manuales, nunca las hacen) hasta la posible validación o restablecimiento.

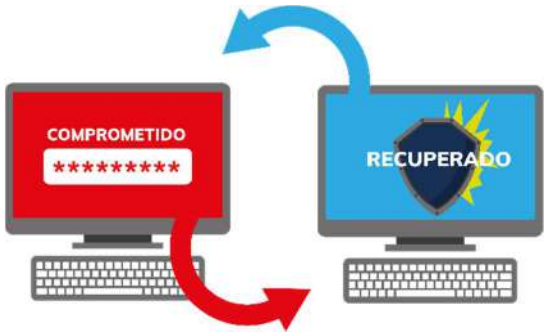
Replicar: en el proceso de replicación, para que siempre lo puedas recordar cuenta hacia atrás, 3, 2, 1, el **número tres** significa realizar 3 copias de seguridad, la original y dos adicionales, mientras más copias de seguridad tengas, menos opciones de perder tus activos.

El **número dos** significa, almacena **dos copias en dos medios diferentes**, estos medios pueden ser, discos duros, cintas, equipos NAS, o el dispositivo que gustes, siempre y cuando no sean los mismos medios, ya que, si almacenas en el mismo medio las copias de seguridad, cabe la posibilidad de que se dañen de la misma forma y pierdas todo.

El **número uno** significa, una copia de seguridad en **un lugar distinto, remoto o fuera de sitio**, imagina que el edificio se cae o se inunda, o un ladrón entra y roba el medio de almacenamiento principal, es posible que todas tus copias de seguridad se pierdan si están en un mismo lugar, por ello, es necesario tener una copia de seguridad fuera del sitio principal, por si se llega a presentar un caso extremo. **Recuerda La ley de Murphy.**

Restablecer: es importante hacer pruebas, no esperes hasta que algo falle en tus sistemas, y hasta ese día darte cuenta que los respaldos no funcionan o te hace falta algún complemento para restablecer tus operaciones, esto te dará múltiples ventajas.

- Te ayudará a conocer el tiempo de restablecimiento que puede tomarte en un ambiente de fallo real.
- Conocer los recursos (tiempo, equipo, accesorios, servicios, etc.) que necesitarás para poder restablecer tus operaciones.
- Te ayudará a identificar si hay problemas de restablecimiento por daño o incompatibilidad, esto te permitirá corregir problemas antes de que suceda un problema, y corregirlos.



Si requieres más información o apoyo para poder implementar estos puntos en tu organización, podemos ayudarte.

¿Cómo podemos desarrollar esto?

Microsoft "Backup and Restore": herramienta para copias de seguridad instalada en los sistemas operativos Microsoft®. **Referencia**: (https://support.microsoft.com/en-us/help/17127/windows-back-up-restore)

Apple Time Machine: herramienta de copia de seguridad instalada en los sistemas operativos Apple® (https://support.apple.com/en-us/HT201250)

Bacula: solución de recuperación y respaldo de red basado en código abierto (http://blog.bacula.org/)

Macrium Software: Solución de copia de seguridad basada en imagen o Bare-metal, lo puedes descargar a través del siguiente enlace: (https://www.macrium.com/reflectfree)

Referencia de control

- **ISO/IEC 27001:2013 -** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3
- **NIST -** PR.IP-4:

Cifrado de información

Día 7

¿Por qué es importante el cifrado?

Los dispositivos pueden perderse, ser robados o interceptados en sus comunicaciones, por eso es necesario **cifrar la información tanto a nivel de dispositivo, a nivel de archivo**, de ser posible, y a nivel de transmisión de información mediante el uso de una VPN.

Puedes hacer uso **de aplicaciones o herramientas de terceros** que te permitan tener la gestión del cifrado de dispositivos, esto te facilitará en tu despliegue de cifrado, ejemplo de esto, una solución de seguridad **endpoint o appliance**, si no hay tanto presupuesto podemos utilizar **Bitlocker**, ¡pero cuidado! Si olvidas la contraseña, será un problema volver a recuperar la misma, si no guardas bien el código de recuperación.

Al implantar la política de cifrado de la organización, deberían tenerse en cuenta las regulaciones y restricciones nacionales que puedan resultar aplicables al uso de técnicas criptográficas en las distintas partes del mundo, así como a las cuestiones relativas al flujo transfronterizo de información cifrada

¿Qué debemos de obtener de esto?

Tomar una decisión en cuanto a si una solución criptográfica resulta adecuada debería considerarse como parte del proceso general de evaluación de riesgos y selección de controles. En ese caso, esta evaluación podría utilizarse para determinar si un control de cifrado es adecuado, qué tipo de control debería aplicarse, para qué fin y en qué procesos de negocio.

La política sobre el uso de controles de cifrado resulta necesaria para maximizar los beneficios y minimizar los riesgos de utilizar técnicas criptográficas, así como para evitar un uso inadecuado o incorrecto.

Debería consultarse con un especialista al seleccionar los controles de cifrado que sean apropiados para cumplir con los objetivos de la política de seguridad de la información.

Referencia de control

- **ISO/IEC 27001:2013 -** A.10.1

Protección de activos BYOD

Díg 8

El teletrabajo abrió la puerta a el uso de los recursos personales de los usuarios para realizar las actividades laborales, desde el servicio de internet, computadora, almacenamiento, etc.

Cuando se utilicen dispositivos móviles, se debería tener un cuidado especial para asegurar que no se compromete la información del negocio. Una política de dispositivos móviles debería tener en cuenta los riesgos de trabajar con dispositivos en entornos desprotegidos, como lo es fuera de la red de la organización, como lo son zonas públicas, salas de reunión, las casas y otras áreas desprotegidas fuera de las instalaciones de la organización.

Dentro de estos medios se debería implantar algún tipo de protección para evitar el acceso no autorizado o la revelación de la información almacenada y procesada por estos dispositivos, por ejemplo, utilizando técnicas de cifrado (véase el día 7) e imponiendo el uso de protocolos secretos de identificación y autenticación

Como recomendación, podemos **mencionarte no hacer uso de equipos personales** de los usuarios para realizar trabajo remoto, a menos que tengas **políticas de BYOD** implementadas en la organización, por temas legales, suele ser más complicado gestionarlos ya que podemos invadir la privacidad del usuario, sí es el único dispositivo disponible y se tiene **consentimiento del usuario**, asegúrate de tener ese consentimiento por escrito en **contrato,** en este contrato deberán incluirse las **aplicaciones a instalar, servicios a utilizar, modo de trabajo** desde el equipo, **recursos a los que se tendrá acceso y medidas de seguridad** (protocolos, procesos, cifrado y tecnologías, etc.) que se implementarán para salvaguardar la información de nuestra empresa.

Si el presupuesto lo permite, bríndales los **equipos de la empresa a los usuarios** para trabajar de forma remota (no sin antes haber aplicado un proceso de hardening). El configurar y entregar los dispositivos de la empresa nos brindará una mejor seguridad para nuestra información al momento de que el usuario trabaje sin importar el lugar donde realice sus actividades, ya que disponemos de la autoridad total del dispositivo.

¿Qué debemos de obtener de esto?

Se debe obtener un listado de todos los equipos de red, servidores, pc, dispositivos móviles con el detalle de su número de serie, fabricante, garantía, proveedores, factura, también se deben de incluir un listado de los softwares instalados para prevenir que software no permitido sea utilizado en la organización.

Referencia de control

- **ISO/IEC 27001:2013 -** A.6.2.1

Hardening para dispositivos de red

Día 9

Es importante, implementar y gestionar activamente (rastrear, reportar, corregir) la configuración de seguridad, de puertos, protocolos y servicios en dispositivos e infraestructura de red y controlar de forma rigurosa los cambios para para minimizar las ventanas de vulnerabilidad disponibles para los atacantes.

¿Por qué es importante el inventario de activos?

Como mencionábamos en el punto del día dos, la mayoría de los fabricantes de dispositivos, no realizan pre configuraciones de seguridad, sólo mantienen configuraciones por defecto para todos sus dispositivos

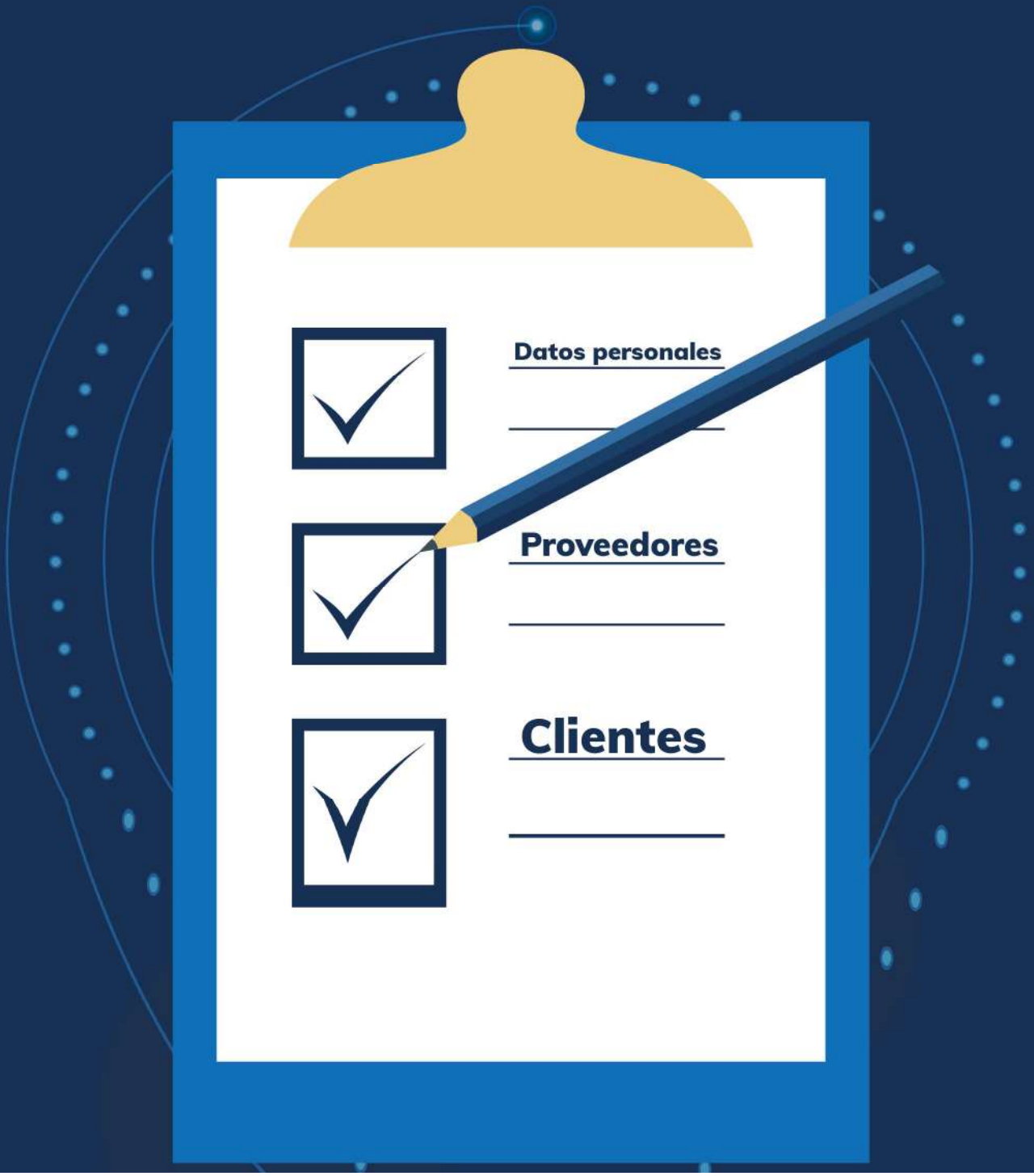
¿Cómo podemos desarrollar esto?

No cambiará mucho lo mencionado contra el punto del día dos las recomendaciones que te hagamos, sin embargo, te comentamos que habrá un punto diferente, y es la revisión de un marco de referencia para que puedas hacer uso de él, y así mejorar la seguridad de dispositivos conectados a internet o que conformen parte operativa de tu red.

Qué herramientas podemos utilizar:

OpenVAS – Esta es una herramienta de open source que puedes descargar desde el siguiente enlace: https://openvas.org/
Microsoft Baseline Security Analyzer – es una herramienta de seguridad de Microsoft que nos permite desarrollar una línea base de seguridad, enlace de descarga: https://www.microsoft.com/en-us/download/details.aspx?id=19892
GFI Lan Guard – es una herramienta de seguridad que te permite comprobar los ordenadores donde comprobará todas las contraseñas, los puertos abiertos, las entradas de registro e incluso las conexiones de red inalámbricas: https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard

Protección de Datos



Día 10

¿Qué son los datos personales?

Tomando en cuenta el RGPD de la unión europea, podemos considerar los datos personales son cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal.

Los datos personales que hayan sido anonimizados, cifrados o presentados con un seudónimo, pero que puedan utilizarse para volver a identificar a una persona, siguen siendo datos personales y se inscriben en el ámbito de aplicación del RGPD.

Los datos personales que hayan sido anonimizados, de forma que la persona no sea identificable o deje de serlo, dejarán de considerarse datos personales. Para que los datos se consideren verdaderamente anónimos, la anonimización debe ser irreversible.

¿Por qué es importante la protección de datos?

Dentro de cada país suele existir una regulación que nos obliga a proteger de forma legal los datos personales, algunas son derivados de la anterior LOPD 15/1999 o de su homologo más reciente que es el RGPD, dentro de estos marcos de protección de datos suelen encontrarse textos similares a los siguientes:

Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo, se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.

El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.

Textos obtenidos de la LFPDPPP 5 de julio de 2010.

¿Cómo podemos desarrollar esto?

Para cumplir con la legislación nacional, te recomendamos apoyarte con una persona especialista, de preferencia un abogado especializado en protección de datos personales, ya que ellos serán los encargados de generar la documentación necesaria para evitar que puedas caer en incumplimiento de políticas o procedimientos y seas acreedor de sanciones por parte de la unidad reguladora de tu país, sin embargo, también deberás hacer uso de personal especializado en tecnología para proteger los datos personales de forma técnica con base en las recomendaciones de.

Te recomendamos darle un vistazo a un Playlist en nuestro canal de Youtube del instituto de ciberseguridad llamado Jornada de Protección de datos personales, en el que hablamos a detalle de todo lo referente que debemos cumplir con base en esta especialidad, mismo que te compartimos: **https://youtu.be/4APu4hmYMgE.**

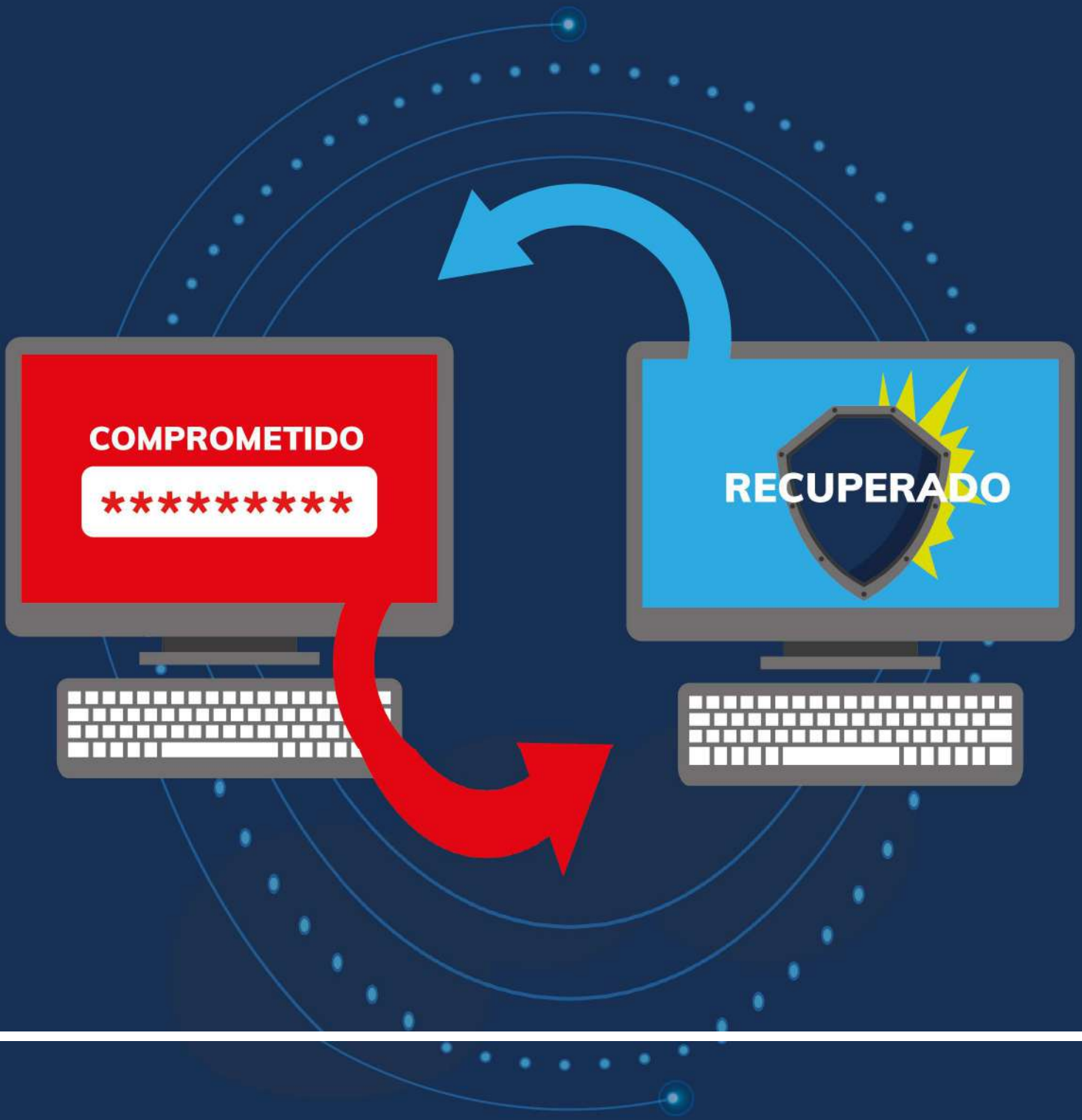
Con base en las leyes de protección de datos, también se puede tomar como punto de partida de la ciberseguridad en la organización, usándola como marco de referencia para su implementación, sin embargo, la especialidad está completamente basada en la protección de la información que es de carácter personal y que es almacenada en los dispositivos electrónicos o que existe en algún archivero, ya que las legislaciones contemplan la parte digital y física.

En el instituto de Ciberseguridad, te podemos ayudar con esto, contamos con personal especialista en protección de datos en ambas reformas LOPD 15/1999 y RGPD.

Referencia de control

- **ISO/IEC 27001:2013 -** A.18.1.1, A.18.1.4

Gestión y respuesta a incidentes



Día 11

“Se puede perdonar el ser derrotado, pero nunca el ser sorprendido”. Federico I, “el Grande”, de Prusia

Todo sistema es vulnerable, eso es inevitable, por ello para proteger la información de la organización, se debe contar con una infraestructura de respuesta a incidentes (por ejemplo, planes, funciones definidas, capacitación, comunicaciones, supervisión de la gestión) para identificar, responder, contener y restablecer tu operación de manera efectiva ante cualquier tipo de incidente o atacante, restaurando la integridad de la operación del negocio y evitando pérdidas económicas considerables.

¿Por qué es importante el inventario de activos?

Cuando un incidente ocurre, y si no se cuenta con un plan de respuesta a incidentes, la cantidad de presión en el momento, será inmensa, por ello es importante desarrollar procedimientos correctos, informes, recopilación de datos, responsabilidad de gestión, protocolos legales y estrategia de comunicaciones que permitan a la organización comprender, gestionar y recuperarse de potenciales incidentes informáticos.

Si la organización no cuenta con un plan de respuesta a incidentes, será muy complicado detectar, contener, erradicar y recuperarnos de forma correcta una potencial amenaza o atacante, generando posibles daños irreversibles en la organización, ya que no habría una estrategia para minimizar los daños y generando un impacto mayor del que pudo haberse previsto.

¿Cómo podemos desarrollar esto?

Es importante comprender que esto se trata de una metodología, no de un software que permita realizar todo, aunque existen soluciones EDR en el mercado, que prometen el sol y la luna respecto a protección, tenemos que comentarte que estas soluciones no te protegerán del todo, ya que las amenazas no sólo son tecnológicas, hay amenazas naturales, humanas, electrónicas, etc.

Por lo tanto, te invitamos a contactar a uno de nuestros especialistas, él te podrá asesorar sobre qué pasos son los que debemos seguir para generar tu estrategia de respuesta a incidentes.

¿Qué debemos de obtener de esto?

- Una estrategia, política, planes y procedimientos de respuesta a incidentes.
- Definición de la gravedad y clasificación del incidente.
- Desarrollo y capacitación de un equipo de respuesta a incidentes.
- Establecer una cadena de mando y procedimientos de notificación.

Referencia de control

- **ISO/IEC 27001:2013 -** A.16
- **NIST –** segmento de control de respuesta a incidentes (RS.XX)

Programa de capacitación y concienciación sobre seguridad

Día 12

Lo sabemos, los usuarios siempre son uno de los puntos más críticos en la seguridad, y prácticamente todo lo que te hemos dicho anteriormente, no serviría de nada si los usuarios no forman parte activa de lo que nosotros llamamos "**La primera línea de defensa**", como consultores y especialistas en concienciación y culturización de usuarios podemos entregarte un par de recomendaciones que sabemos te serán útiles, como a nosotros tan efectivas al momento de realizar estos planes de capacitación, y hacer que tus usuarios sean eso, un medio de defensa preventiva en vez de un cumulo de futuros problemas a la seguridad.

La ciberseguridad no se trata solo de tecnología; También se trata de procesos y personas. Tener solo herramientas y software de seguridad no es suficiente. Para ayudar a proteger su organización, sus empleados y el personal también deben practicar comportamientos de seguridad cibernética fuertes. Hay dos consideraciones clave para "proteger cibernéticamente" a su personal: lo que usted comunica y cómo se comunica.

¿Qué comunicar?

- Identifique a las personas dentro de su organización que tienen acceso o que manejan datos confidenciales, y asegúrese de que entiendan su papel en la protección de esa información.
- Métodos de ataque comunes como correo electrónico de phishing y ataques de llamadas telefónicas. Asegúrese de que sus empleados puedan explicar e identificar indicadores comunes de un ataque.
- Asegúrese de que todos sepan que el sentido común es, en última instancia, su mejor defensa. Si algo parece extraño, sospechoso o demasiado bueno para ser verdad, lo más probable es que sea un ataque.
- Fomentar el uso de claves fuertes y únicas para cada cuenta y / o verificación en dos pasos cuando sea posible.

¿Cómo comunicarlo?

- **1.- Realiza simulaciones de seguridad:** esto te permitirá conocer cuáles son los usuarios y la posible amenaza a la que son más propensos a ser afectados (ingeniería social, infección por malware, robo de información, etc)
- **2.- Crear el plan de capacitación**: Una vez identificado el problema, es necesario comenzar a realizar los contenidos que se utilizarán, esto se debe hacer en base a la información recabada en el punto anterior.
- **3.- Impartir la capacitación o contenido:** Una vez teniendo el contenido, es necesario comenzar a distribuirlo a los usuarios.
- **4.- Evaluar:** este punto es para validar si los usuarios han mejorado o no en las áreas de oportunidad identificadas.