economistas
Consejo General

ReDigital economía y transformación digital

REA auditores

FICHA 01 22

grupo de trabajo de auditoría

SEPTIEMBRE 2022

Medidas de protección de los sistemas informáticos

La transformación digital llevada a cabo por las entidades auditadas exige una evolución en el mismo sentido de los auditores de cuentas con objeto de incrementar la calidad de los trabajos, evaluar mejor los riesgos cada vez más amplios de las entidades auditadas, mejorar la eficiencia del trabajo al reducir tareas de poco valor y desplegar acciones que permitan captar y retener el talento.

Respecto al cumplimiento normativo, se han introducido importantes requerimientos en el Reglamento de la Ley de Auditoría que afectan a la forma de trabajar de los auditores a partir del 1 de julio de 2022. Citamos algunos de ellos: la obligación de que todos los papeles de trabajo sean en formato electrónico, con las debidas medidas de seguridad que garanticen su autenticidad; la digitalización de toda la documentación existente en formato papel; procedimientos que aseguren la custodia, integridad y recuperación de la información; garantizar la accesibilidad y autorización restringida para su acceso; y realizar de forma rutinaria copias de seguridad en formato digital en diferentes momentos y, al menos, una vez al año. Todos ellos son retos a los que se enfrenta la actividad profesional.

Se observa, por lo tanto, una exigencia de modernización tecnológica de los despachos de auditoría que es prioritaria y estratégica, teniendo en cuenta la función de interés público de la actividad profesional de la auditoría de cuentas.

Desde el grupo de trabajo de auditoría de ReDigital publicaremos periódicamente estas fichas para ayudar a los auditores de cuentas a cumplir con la normativa y, a su vez, mejorar la eficiencia y eficacia en su trabajo diario.

De acuerdo con el artículo 66.4 del Real Decreto 2/2021, de 12 de enero, por el que se aprueba el Reglamento de desarrollo de la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas, los auditores de cuentas deben disponer de procedimientos y medidas de protección de los sistemas informáticos.

> "4. Los procedimientos administrativos relativos a la identificación, valoración y respuesta a los riesgos que puedan afectar a la actividad de la auditoría de cuentas **incluirán** los relativos al **control y la protección de los sistemas informáticos,** al **tratamiento de datos personales**, así como, en el caso de los **auditores de entidades de interés público,** aquellos que permitan **asegurar** la continuidad y regularidad de la actividad de auditoría de cuentas, que incluirán:
>
> - La realización de evaluaciones cualitativas y cuantitativas sobre los posibles impactos, tanto de factores internos como externos, en dicha continuidad.
> - El diseño e implementación de planes de contingencias y de continuidad, que formarán parte del marco de gestión de riesgos de los auditores de cuentas.
> - Dichos planes serán objeto de revisión periódica al menos anualmente."

Por otra parte, el Artículo 68. Proporcionalidad y requisitos simplificados, establece:

> "1. Las normas a que se refieren los artículos 66 y 67 establecerán que la **organización interna y su documentación justificativa sean proporcionados a la dimensión y estructura organizativa** de los auditores de cuentas y acorde con las características, complejidad y volumen de los trabajos de auditoría".

A CONTINUACIÓN SE PROPONEN UNA SERIE DE PROCEDIMIENTOS QUE PUEDEN IMPLEMENTARSE POR EL AUDITOR DE CUENTAS O LA SOCIEDAD DE AUDITORÍA

Para dar respuesta a los criterios exigidos en los artículos anteriores se proponen una serie de procedimientos que pueden implementarse por la firma de auditoría:

Modelo propuesto de documentación justificativa

XXX AUDITORES ha establecido un conjunto de controles administrativos relativos a la identificación, valoración y respuesta a los riesgos que puedan afectar la actividad de la auditoría de cuentas relativos al control y protección de los sistemas informáticos.

Para dar respuesta a dichos riesgos la firma de auditoría (o auditor individual), establece primeramente un marco de riesgos de tecnologías de la información (en adelante, TI) que busca reducir el impacto en la organización si un riesgo se materializa, o bien reducir la probabilidad de su ma-

terialización si excede de los niveles de riesgo aceptable. Para determinar el "nivel de riesgo aceptable" de la organización se considera el artículo 68.1 del RLAC, en los relativo a la dimensión y estructura organizativa de los auditores de cuentas y acorde con las características, complejidad y volumen de los trabajos de auditoría.

ALCANCE

El riesgo relacionado con las TI es una condición esencial del negocio y puede suponer:

- Pérdida de información.
- Interrupción de la actividad.
- Pérdida de ingresos.
- Daños en equipos e instalaciones informáticas o controladas por éstas.
- Carencia de autenticidad de las comunicaciones.
- Daños reputacionales.
- Afrontar acciones legales.

Involucra multitud de características y tecnologías especializadas:

- Agentes de la amenaza.
- Errores humanos.
- Vectores de ataque.
- Fallos de control.
- Vulnerabilidades de software, …

Para dar respuesta a los riesgos, primero hay que determinar la probabilidad de un evento y su impacto sobre la organización, así como su efecto sobre las dimensiones de la seguridad:

- Disponibilidad.
- Autenticidad.
- Integridad.
- Confidencialidad.
- Trazabilidad.

Para a continuación:

- Obtener el escenario de riesgo.
- Asegurar que los escenarios de riesgo sean relevantes y estén vinculados con el riesgo real del negocio.
- Integrar la práctica de riesgos de TI en los procesos y las actividades rutinarias.
- Adoptar un planteamiento consistente que sea estándar, repetible y esté alineado con la actividad de auditoría de cuentas.
- Medir la capacitación de la organización: indicador de la aptitud para realizar actividades relacionadas con TI.

El enfoque propuesto para garantizar razonablemente el cumplimiento del artículo 66.4 e incluso del artículo 69.1 del RLAC, en lo relativo a mitigar los riesgos de TI en las firmas de auditoría de cuentas, es recurrir al marco conceptual establecido por el *Center for Internet Security* (CIS)[1] que prioriza y clasifica los controles de TI según su importancia para hacer frente a las ciber-amenazas.

Dichos controles, pensados para organizaciones de cualquier tipo, establecen un subconjunto reducido de los controles generales de ciberseguridad y clasifican a sus seis primeros como controles básicos. A estos ha sido incorporado el control de copias de seguridad de datos y sistemas al ser un elemento fundamental para mantener un grado razonable de ciber-resiliencia.

CONTROLES BÁSICOS

1. Inventario y control de dispositivos físicos.
2. Inventario y control de software autorizado y no autorizado.
3. Proceso continuo de identificación y remediación de vulnerabilidades.
4. Uso controlado de privilegios administrativos.
5. Configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores.
6. Registro de la actividad de los usuarios.
7. Copias de seguridad de datos y sistemas.

1. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS

RECOMENDACIÓN

Disponer de un inventario de los elementos físicos que componen los sistemas de información (en adelante, SI), de la firma es un requisito indispensable para la identificación de los riesgos relativos al control y la protección de los SI. No puede protegerse de aquello que se desconoce.

1. Ver https://www.cisecurity.org/controls - Referencia a CIS Controls v7

OBJETIVO DE CONTROL

Gestionar activamente (inventariar, revisar y corregir) todos los dispositivos hardware en la red, de forma que sólo los dispositivos autorizados tengan acceso a la red.

Este control permite definir la base de lo que hay que defender. No pueden ser defendidos sin conocer los dispositivos conectados.

El inventario debe ser tan completo como sea posible, mantenerse actualizado, incluir todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que es responsable de las decisiones relativas al mismo.

En cualquier caso, el objetivo inicial del control es conocer lo que está en la red para que pueda ser defendido y, posteriormente, impedir que dispositivos no autorizados se unan a la red.

DISEÑO DEL CONTROL

El inventario debe cubrir todo el dominio de seguridad de los SI, hasta alcanzar los puntos de interconexión y los servicios prestados por terceros. La granularidad debe ser suficiente para cubrir las necesidades de reporte de incidentes y para hacer un seguimiento, tanto formal (auditorías) como reactivo en el proceso de gestión de incidentes.

- **Identificación del activo:** fabricante, modelo, número de serie.
- **Configuración del activo:** perfil, política, software instalado.
- **Software instalado:** fabricante, producto, versión y parches aplicados.
- **Equipamiento de red:** MAC, IP asignada (o rango).
- **Ubicación del activo:** ¿dónde está?
- **Propiedad del activo:** persona responsable del mismo.

2. INVENTARIO Y CONTROL DE SOFTWARE AUTORIZADO Y NO AUTORIZADO

RECOMENDACIÓN

Mantener programas no actualizados (con vulnerabilidades) es uno de los vectores de entrada más utilizados por los atacantes para comprometer los SI. Sin el conocimiento o el control apropiados del software desplegado en una organización, los defensores no pueden asegurar adecuadamente sus activos.

Una vez que una máquina ha sido comprometida, los atacantes la utilizan a menudo como punto para recoger información sensible del sistema en el que está integrada y de otros sistemas conectados a él. Además, las máquinas comprometidas se utilizan como punto de lanzamiento para el movimiento a través de la red y de las redes conectadas (movimiento lateral). De esta manera, los atacantes pueden rápidamente convertir una máquina comprometida en muchas.

El control de todo el software también desempeña un papel fundamental en la planificación y ejecución de copias de seguridad y en la recuperación del sistema.

OBJETIVO DE CONTROL

Gestionar activamente (inventariar, revisar y corregir) todo el software en la red, de forma que sólo se pueda instalar y ejecutar software autorizado y que el no autorizado sea detectado y se evite su instalación y ejecución.

La finalidad de este control es asegurar que sólo está permitido ejecutar software autorizado en los sistemas de la organización impidiendo la ejecución de software potencialmente vulnerable.

Aunque no es una solución mágica para la defensa, este control a menudo se considera uno de los más eficaces para la prevención y detección de ciberataques.

La implementación del control a menudo requiere que las organizaciones reconsideren sus políticas y su cultura, los usuarios ya no podrán instalar el software que deseen. Pero este control está implementado con éxito por numerosas organizaciones, y probablemente ayudará a prevenir y detectar ciberataques.

DISEÑO DEL CONTROL

El inventario debe cubrir todo el dominio de seguridad del SI, hasta alcanzar los puntos de interconexión y los servicios prestados por terceros. La granularidad debe ser suficiente para cubrir las necesidades de reporte de incidentes y para hacer un seguimiento, tanto formal (auditorías) como reactivo en el proceso de gestión de incidentes.

- **Identificación del activo:** fabricante, modelo, número de serie.
- **Configuración del activo:** perfil, política, software instalado.
- **Software instalado:** fabricante, producto, versión y parches aplicados.
- **Equipamiento de red:** Máquina, MAC, IP asignada (o rango) .
- **Ubicación del activo:** ¿dónde está?
- **Propiedad del activo:** persona responsable del mismo.

3. PROCESO CONTINUO DE IDENTIFICACIÓN Y REMEDIACIÓN DE VULNERABILIDADES

RECOMENDACIÓN

El personal responsable de los SI de la firma debe operar en un flujo constante de información nueva: actualizaciones de software, parches, avisos de seguridad, boletines de amenazas, etc. La comprensión y gestión de las vulnerabilidades se ha convertido en una actividad continua, que requiere tiempo, atención y recursos significativos.

Un atacante tiene acceso a la misma información y puede aprovechar las brechas entre la aparición de nuevos conocimientos y la remediación.

Las organizaciones que no escanean las vulnerabilidades y abordan de forma proactiva los defectos encontrados se enfrentan a una alta probabilidad de que sus sistemas informáticos sean comprometidos.

OBJETIVO DE CONTROL

Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.

El objetivo de este control es conocer y eliminar debilidades técnicas que existen en los sistemas de información de la organización, reduciendo la probabilidad de que los sistemas sigan siendo vulnerables.

Las organizaciones deben implementar herramientas de gestión de vulnerabilidades para dotarse de la capacidad de detectar y remediar debilidades de software explotables.

DISEÑO DEL CONTROL

La firma de auditoría debe conocer en todo momento el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

A. Aceptación y puesta en servicio

Previamente a la puesta en servicio se comprobará que:

1. Se cumplen los criterios de aceptación en materia de seguridad.
2. No se deteriora la seguridad de otros componentes del servicio.

B. Gestión de la configuración

Se gestionará de forma continua la configuración de los componentes del sistema de forma que reaccione a las vulnerabilidades reportadas.

C. Mantenimiento

Para mantener el equipamiento físico y lógico se aplicará lo siguiente:

1. Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas.
2. Se efectuará un seguimiento continuo de los informes de defectos (actuación proactiva).
3. Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.

4. USO CONTROLADO DE PRIVILEGIOS ADMINISTRATIVOS

RECOMENDACIÓN

El uso inadecuado de privilegios administrativos es un método primario para que los atacantes se propaguen dentro de una entidad objetivo. Dos técnicas de ataque muy comunes aprovechan los privilegios administrativos incontrolados.

La revisión de este control puede orientarse a verificar la existencia de una política de alta, baja y mantenimiento de usuarios administradores, y la fortaleza de las contraseñas y las tareas que se desarrollan para comprobar su cumplimiento.

OBJETIVO DE CONTROL

Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso, asignación y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.

Este control garantiza que los privilegios de administración de sistemas estén asignados únicamente a los empleados que los necesitan, en base a las funciones que desempeñan, y que la entidad pueda atribuir las acciones administrativas a usuarios individuales.

Desafortunadamente, para facilitar la agilidad y la comodidad, muchas organizaciones permiten que su personal tenga derechos de administrador tanto a nivel de la aplicación de gestión, como en los sistemas que le dan soporte (sistema operativo, base de datos, etc.) así como en sus equipos.

La situación anterior deriva en la existencia del riesgo de acceso y cambios no autorizados a los sistemas, que puede materializarse desde dos puntos diferentes:

- **Desde el punto de vista externo,** cuya puerta de entrada es el usuario, y en el que se aprovechan los privilegios de administración de los usuarios en sus equipos, para acceder desde fuera a la red interna de la entidad.

- **Desde el punto de vista interno,** es decir, desde dentro de la red de la entidad (bien por parte de un empleado con acceso autorizado o bien como consecuencia de un ciberataque que se ha iniciado externamente aprovechando la debilidad descrita en el párrafo anterior).

  En este caso, la gestión inadecuada de los privilegios de administración en los sistemas operativos, base de datos, etc. da a los atacantes la oportunidad de acceder y realizar cambios no autorizados en los sistemas corporativos que sustentan los procesos de gestión.

Este control nos lleva a que las cuentas de usuarios administradores de aplicaciones, bases de datos, sistemas operativos y equipos de usuario deben estar identificadas, su uso auditado, eliminando las que no se utilizan y cambiando las que están definidas por defecto. Adicionalmente, deben cumplir con la política de fortaleza de contraseñas.

DISEÑO DEL CONTROL

A. Control de acceso

El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.

El control de acceso que se implante en un sistema real será un punto de equilibrio entre la comodidad de uso y la protección de la información.

En todo control de acceso se requerirá lo siguiente:

1. Que todo acceso esté prohibido, salvo concesión expresa.
2. Que la entidad, usuario o proceso quede identificado singularmente.
3. Que la utilización de los recursos esté protegida.
4. Que se definan para cada usuario los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo qué autorización.
5. Si es posible la segregación de funciones, diferenciar las personas que autorizan, usan y controlan el uso.
6. Que la identidad del usuario quede suficientemente autenticada.
7. Que se controle tanto el acceso local como el acceso remoto.

Con el cumplimiento de todas las medidas indicadas se garantiza que nadie accede a un recurso sin autorización. Además, quedará registrado el uso del sistema para poder detectar y reaccionar ante cualquier fallo accidental o deliberado.

B. Gestión de los derechos de acceso

Los derechos de acceso de cada usuario se limitarán atendiendo a los siguientes principios:

1. Mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones. De esta forma se acotan los daños que pudiera causar un usuario, de forma accidental o intencionada.
2. Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.
3. Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

C. Mecanismo de autenticación

Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen, pudiendo usarse los siguientes factores de autenticación:

- "Algo que se sabe": contraseñas o claves concertadas.
- "Algo que se tiene": componentes lógicos (tales como certificados software) o dispositivos físicos (en expresión inglesa, *tokens).*
- "Algo que se es": elementos biométricos.

Los factores anteriores podrán utilizarse de manera aislada o combinarse para generar mecanismos de autenticación fuerte.

5. CONFIGURACIONES SEGURAS DEL HARDWARE Y SOFTWARE DE DISPOSITIVOS MÓVILES, PORTÁTILES, EQUIPOS DE SOBREMESA Y SERVIDORES

RECOMENDACIÓN

Los fabricantes y vendedores de tecnología normalmente entregan los productos con las configuraciones predeterminadas para los sistemas operativos y las aplicaciones orientadas a la facilidad de uso y no a la seguridad.

Cuando se entrega un software es habitual encontrarse con controles poco robustos, servicios y puertos abiertos, cuentas o contraseñas predeterminadas, protocolos antiguos (vulnerables), preinstalación de software innecesario; todos estos aspectos son vulnerables en su estado predeterminado (por defecto).

El desarrollo de opciones de configuración con buenas propiedades de seguridad es una tarea compleja más allá de la capacidad de los usuarios individuales, requiriendo a veces competencias complejas para tomar buenas decisiones.

Incluso si se desarrolla e instala una configuración inicial fuerte, ésta debe ser revisada y actualizada asiduamente para evitar el deterioro de la seguridad, en particular cuando el software es actualizado o parcheado, se divulgan nuevas vulnerabilidades de seguridad, o las configuraciones se "ajustan" para permitir la instalación de nuevo software o para dar soporte a nuevos requerimientos operacionales.

Si no se revisa y actualiza de forma continua, los atacantes encontrarán oportunidades para explotar tanto los servicios accesibles a la red como el software cliente.

OBJETIVO DE CONTROL

Establecer una configuración base segura para dispositivos móviles, portátiles, equipos de sobremesa y servidores, y gestionarlas activamente utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir a los atacantes explotar servicios y configuraciones vulnerables.

Por defecto, la mayoría de los sistemas están configurados para facilitar su uso y no necesariamente pensando en la seguridad. Para implantar este control, las organizaciones necesitan reconfigurar los sistemas de acuerdo con estándares de seguridad.

DISEÑO DEL CONTROL

A. Seguridad por defecto

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:

1. El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
2. Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso acreditados.
3. En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, innecesarias e, incluso, aquéllas que sean inadecuadas con el fin que se persigue.
4. El uso habitual del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

B. Configuración de seguridad

Se configurarán los equipos previamente a su entrada en operación, de forma que:

1. Se retiran cuentas y contraseñas estándar.
2. Se aplicará la regla de «mínima funcionalidad»:
   - El sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad.
   - No proporcionará funciones gratuitas, ni de operación, ni de administración, ni de auditoría, reduciendo de esta forma su perímetro al mínimo imprescindible.
   - Se eliminarán o desactivarán mediante el control de la configuración aquellas funciones que no sean de interés, innecesarias e, incluso, las que sean inadecuadas al fin que se persigue.
3. Se aplicará la regla de «seguridad por defecto»:
   - Las medidas de seguridad serán respetuosas con el usuario y le protegerán salvo que se exponga conscientemente a un riesgo.
   - Para reducir la seguridad, el usuario tiene que realizar acciones de forma consciente.
   - El uso habitual en los casos en que el usuario no disponga de la suficiente formación para la utilización del programa será de uso seguro.

C. Gestión de la configuración de seguridad

Se gestionará de forma continua la configuración de los componentes del sistema de forma que:

- Se mantiene en todo momento la regla de "funcionalidad mínima".

- Se mantiene en todo momento la regla de "seguridad por defecto".
- El sistema se adapta a las nuevas necesidades, previamente autorizadas.
- El sistema reacciona a las vulnerabilidades reportadas.
- El sistema reacciona a incidentes.

6. REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

RECOMENDACIÓN

Sin unos *logs* (cuaderno de bitácora que explica el comportamiento del sistema o programa), de auditoría sólidos, un ataque puede pasar desapercibido por tiempo indefinido y los daños infringidos pueden ser irreversibles.

A veces estos registros son la única evidencia de un ataque exitoso. Debido a deficientes o inexistentes procesos de análisis de registros de *logs,* los atacantes controlan a veces máquinas víctima durante meses o años sin que nadie se percate de la intrusión en la organización, a pesar de que la evidencia del ataque ha quedado registrada en dichos registros que no han sido examinados.

OBJETIVO DE CONTROL

En entidades de reducido tamaño, es recomendable que este control se apoye en las *suites* de seguridad (léase programas para la prevención, detección y respuesta ante amenazas), para recoger, gestionar y analizar *logs* de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.

Para que sea eficaz, todos los sistemas (dispositivos móviles, estaciones de trabajo y servidores, físicos o virtuales), deberán tener desplegada la herramienta de protección que mantiene información sobre los factores de riesgo mediante la detección y priorización de las configuraciones erróneas del software y del sistema operativo, así como tener definidas acciones de alerta ante una detección o un ataque.

DISEÑO DEL CONTROL

La industria proporciona numerosas herramientas para la prevención, detección y respuesta ante amenazas, algunas de estas herramientas de propósito empresarial son:

- Acronis Cyber Protect.
- Avast Business.
- AVG Business.
- Avira Protection Cloud.
- Bitdefender GravityZone Business Security.
- BullGuard Premium Protection.
- ESET Endpoint Antivirus.
- Intego.
- Kaspersky.
- Malwarebytes for Teams.
- McAfee Security for Business.
- Norton Small Business.
- Panda Endpoint Protection Plus.
- Vipre Core Defense.
- Windows Defender (Azure).

A CONSIDERAR:

- Los programas gratuitos no proporcionan una protección integral.
- Es recomendable la utilización del mismo programa en toda la organización.
- Una gestión de consola centralizada facilita la instalación y la supervisión de los eventos de seguridad de la organización.
- Los informes y alertas accesibles desde una única consola de gestión ayudan a controlar cualquier evento de seguridad.

7. COPIAS DE SEGURIDAD DE DATOS Y SISTEMAS

La importancia de este control es fundamental para mantener un grado razonable de ciber-resiliencia. Si todos los controles preventivos fallan y un ciberataque traspasa todas las líneas de defensa y tiene éxito, el último recurso de la entidad atacada es restaurar sus sistemas y datos en un plazo predeterminado para poder continuar prestando sus servicios.

Este carácter de "último bastión" para la continuidad de la organización ha motivado considerar la necesidad de dedicarle un punto específico que será objeto de desarrollo en próximas fichas cuya publicación os anunciaremos puntualmente.

CONCLUSIÓN

La respuesta al riesgo

Entre los criterios exigidos por el artículo 66.4 e incluso el 69.1 del RLAC, la firma de auditoría por medio de un proveedor de tecnología, en su caso, debe asegurar la garantía razonable de que los datos, la información financiera y los activos de los sistemas de información cumplen las dimensiones de la seguridad (Disponibilidad, Autenticidad, Integridad, Confidencialidad y Trazabilidad).

Para ello, la firma de auditoría debe alinear la implementación de los siete controles básicos de ciberseguridad a sus propias características y riesgos para garantizar razonablemente el control y la protección de los sistemas informáticos, la seguridad en el tratamiento de los datos personales, y la continuidad y regularidad de la actividad de auditoría de cuentas.

REFERENCIAS

- ISACA 2020 - Marco de riesgos de TI (2ª edición)
- https://www.cisecurity.org/controls - Referencia a CIS Controls v7
- Guía práctica de fiscalización de los OCEX – GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad (https://asocex.es/normativa/)
- MOI del REA-Auditores de junio 2022
- https://www.incibe.es/protege-tu-empresa/guias