ESTUDIO DE CASO: “SIMÓN: PARTE II”  
ACTIVIDAD III

DICKSON ARLEY GARCIA RINCON

SENA

SERVICIO NACIONAL DE APRENDIZAJE

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

MEDELLÍN

2019

**INTRODUCCIÓN**

En continuidad con el estudio del caso Simón, se identificaran los diferentes activos presentes y se alinearan las modificaciones resaltadas en la evaluación del informe I de caso Simón. También de nombraran las normas de seguridad informática recomendadas para el caso de estudio en base a la Disponibilidad, Integridad y Confiabilidad.

**ACTIVOS DE INFORMACIÓN**

Se define activo a todo aquello que tiene un valor, en el caso de activos de información, incluye toda información estructurada y no estructurada, es el inventario de todos los equipos informáticos también de la información que se encuentra almacenada en forma escrita, impresa o en base de datos.

**Inventario de activos**

El inventario de activos conforma el primer elemento de la cadena en un sistema de gestión de la seguridad de un sistema. Un inventario de activos se define como una lista de todos aquellos recursos (físicos, software, documentos, servicios, personas, instalaciones) que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. Es necesario tener el inventario de activos para mantener un control sobre los activos y saber en caso de pérdidas que activos fueron afectados, también el tener un inventario actualizado ayuda a la toma de decisiones y mejoras en los sistemas de seguridad.

Todo activo e información debe estar asociado a un propietario quien sería el responsable de su control, producción, desarrollo, mantenimiento, uso y seguridad de los mismos. Algunos entes que pueden intervenir en la interacción con los activos son: Propietario de información, Custodio técnico, Usuario.

La información recopilada en un inventario de activos depende según el alcance y las responsabilidades, también varía de acuerdo a la organización. Existen herramientas especializadas en el control de inventario que ayudan a la actualización constante de la información y de los componentes de cada equipo, también un registro del propietario y usuario a cargo.

**Clasificación de los activos**

Para la clasificación de activos, la norma ISO27001 nos dice que todos los activos de información deben ser identificados de una forma clara y se tiene que realizar y mantener un inventario en el que aparezcan todos los activos de información importantes. Para el caso de estudio de Simón II tenemos los siguientes activos:



PC 1

PC 2

PC 6

PC 5

PC 4

PC 3

Router

Smart Phone

Ethernet

Firewall

Web Service

Impresora

Switch

Server

Tomando en cuenta que en el anterior informe se propuso tipología estrella, se adaptó la imagen de los equipos designados en el ejercicio del caso de estudio.

**Activos Puros:**

* Datos digitales: son archivos, bases de datos, documentación del sistema, manuales de usuarios, material de formación, procedimientos, planes de continuidad, configuración de soporte.
* Activos de software: software de aplicación, software del sistema, herramientas y programas de desarrollo.
* Activos intangibles: reputación, imagen de la organización, ética, licencias, conocimientos técnicos.

**Activos físicos**

* Infraestructura: Edificio, armario (racks) de red o cableado, escritorios, cajones, archivadores, salas de almacenamiento de medios físicos y caja de seguridad, dispositivos de identificación y autentificación, circuito cerrado de televisión (CCTV).

|  |  |  |  |
| --- | --- | --- | --- |
| **Serial de la empresa** | **Serial externo** | **Nombre Equipo** | **Empresa** |
| SMN11 | FFGPRWX1 | Gabinete Rack De Piso | SIMON |
| **Propietario** | **Grupo** | **Ubicación** | **Descripción** |
| SIMON | \SIMON | Medellín | Gabinete Rack |

|  |  |  |  |
| --- | --- | --- | --- |
| **Serial de la empresa** | **Serial externo** | **Nombre Equipo** | **Empresa** |
| SMN12 | JJGPRWX2 | Archivador Cajonera | SIMON |
| **Propietario** | **Grupo** | **Ubicación** | **Descripción** |
| SIMON | \SIMON | Medellín | Mueble color negro |
| **Serial de la empresa** | **Serial externo** | **Nombre Equipo** | **Empresa** |
| SMN13 | JJGPRWR3 | Silla Oficina Escritorio | SIMON |
| **Propietario** | **Grupo** | **Ubicación** | **Descripción** |
| SIMON | \SIMON | Medellín | Silla Oficina Escritorio Reclinable Negra de Malla |

|  |  |  |  |
| --- | --- | --- | --- |
| **Serial de la empresa** | **Serial externo** | **Nombre Equipo** | **Empresa** |
| SMN14 | SEGPRWR3 | Cámaras De Seguridad | SIMON |
| **Propietario** | **Grupo** | **Ubicación** | **Descripción** |
| SIMON | \SIMON | Medellín | Cámaras De Seguridad Kit Cctv 720p Dvr 4 |
| **Fecha Activación** | **Tipo** | **Fabricante** | **Serie** |
| dd/mm/yyyy | Seguridad | Dahua | 793HRX7DNTV |

Valoración: Los activos físicos de infraestructura, contienen información relevante de la empresa y ayudan con la seguridad de la misma. Los archivadores pueden contener archivos impresos de alta confiabilidad. El rack almacena y protege el servidor y el cableado de red así como también organiza la estructura. El acceso al servidor debe ser restringido para prevenir que personas ajenas realicen cambios o eliminen información. Como medida preventiva a eventos de catástrofe natural, se puede hacer un respaldo en servicios en la nube. La información se puede centralizar en el servidor a través de un mapeo de red y luego el servidor subirla a un respaldo en la nube, con esta medida se puede resguardar la información de pérdidas por catástrofe.

* Hardware: Dispositivos de almacenamiento y cómputo como computadoras de escritorio, estaciones de trabajo, portátiles, servidores, módems, impresoras.

|  |  |  |  |
| --- | --- | --- | --- |
| **Serial de la empresa** | **Serial externo** | **Nombre Equipo** | **Empresa** |
| SMN01 | XWOPRWX1 | iMac de Usuario1 | SIMON |
| **Propietario** | **Grupo** | **Ubicación** | **Descripción** |
| Usuario 1 | \SIMON | Medellín | Equipo usuario 1 |
| **Dirección IP** | **Tipo** | **Fabricante** | **Serie** |
| 192.168.0.11 | Workstation | Apple Computer Inc. | C02KDWX7DNCV |
| **Deshabilitado** | **Origen** | **Fecha Activación** | **Fecha Modificación** |
| No | Manual | dd/mm/yyyy | dd/mm/yyyy |
| **Memoria** | **Capacidad de disco** | **Modelo CPU** | **Cargo** |
| 16384.0 | 1 T | Intel Core i5 | Empleo1 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Serial de la empresa** | **Serial externo** | **Nombre Equipo** | **Empresa** |
| SMN02 | XWOPRWX2 | iMac de Usuario2 | SIMON |
| **Propietario** | **Grupo** | **Ubicación** | **Descripción** |
| Usuario 1 | \SIMON | Medellín | Equipo usuario 2 |
| **Dirección IP** | **Tipo** | **Fabricante** | **Serie** |
| 192.168.0.12 | Laptop | Apple Computer Inc. | C02KDWX7DFFV |
| **Deshabilitado** | **Origen** | **Fecha Activación** | **Fecha Modificación** |
| No | Manual | dd/mm/yyyy | dd/mm/yyyy |
| **Memoria** | **Capacidad de disco** | **Modelo CPU** | **Cargo** |
| 16384.0 | 1 T | Intel Core i5 | Empleo2 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Serial de la empresa** | **Serial externo** | **Nombre Equipo** | **Empresa** |
| SMN03 | XWOPRWX3 | HP de Usuario1 | SIMON |
| **Propietario** | **Grupo** | **Ubicación** | **Descripción** |
| Usuario 1 | \SIMON | Medellín | Equipo usuario 3 |
| **Dirección IP** | **Tipo** | **Fabricante** | **Serie** |
| 192.168.0.13 | Workstation | Hewlett-Packard | MXL31506XTT |
| **Deshabilitado** | **Origen** | **Fecha Activación** | **Fecha Modificación** |
| No | Manual | dd/mm/yyyy | dd/mm/yyyy |
| **Memoria** | **Capacidad de disco** | **Modelo CPU** | **Cargo** |
| 16384.0 | 1 T | Intel Core i5 | Empleo3 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Serial de la empresa** | **Serial externo** | **Nombre Equipo** | **Empresa** |
| SMN04 | XWOPRWX4 | Proliat ML350E | SIMON |
| **Propietario** | **Grupo** | **Ubicación** | **Descripción** |
| SIMON | \SIMON | Medellín | Equipo Server 1 |
| **Dirección IP** | **Tipo** | **Fabricante** | **Serie** |
| 192.168.0.14 | Workstation | Hewlett-Packard | MX2416020GG |
| **Deshabilitado** | **Origen** | **Fecha Activación** | **Fecha Modificación** |
| No | Manual | dd/mm/yyyy | dd/mm/yyyy |
| **Memoria** | **Capacidad de disco** | **Modelo CPU** | **Cargo** |
| 16384.0 | 4 T | Intel Core i5 | Server |

|  |  |  |  |
| --- | --- | --- | --- |
| **Serial de la empresa** | **Serial externo** | **Nombre Equipo** | **Empresa** |
| SMN05 | XWOPRWX5 | 3COM Baseline | SIMON |
| **Propietario** | **Grupo** | **Ubicación** | **Descripción** |
| SIMON | \SIMON | Medellín | Switch 2928 |
| **Dirección IP** | **Tipo** | **Fabricante** | **Serie** |
| 192.168.0.1 | Switch | Hewlett-Packard | 926FC3P98439B |
| **Deshabilitado** | **Origen** | **Fecha Activación** | **Fecha Modificación** |
| No | Manual | dd/mm/yyyy | dd/mm/yyyy |
| **Memoria** | **Capacidad de disco** | **Modelo CPU** | **Cargo** |
| - | - | - | SW |

|  |  |  |  |
| --- | --- | --- | --- |
| **Serial de la empresa** | **Serial externo** | **Nombre Equipo** | **Empresa** |
| SMN06 | XWOPRWX6 | HP LaserJet Pro | SIMON |
| **Propietario** | **Grupo** | **Ubicación** | **Descripción** |
| SIMON | \SIMON | Medellín | HP M426fdw |
| **Dirección IP** | **Tipo** | **Fabricante** | **Serie** |
| 192.168.0.16 | Impresora | Hewlett-Packard | 210235A0F2H10 |
| **Deshabilitado** | **Origen** | **Fecha Activación** | **Fecha Modificación** |
| No | Manual | dd/mm/yyyy | dd/mm/yyyy |
| **Memoria** | **Capacidad de disco** | **Modelo CPU** | **Cargo** |
| - | - | - | Impresora |

Valoración de activos: En cuanto al hardware, cada usuario asignado a un equipo es el responsable por la integridad. Se debe implementar contraseñas seguras para que otros usuarios que no están autorizadas puedan acceder a esta información. En caso de pérdidas de información por daño de hardware como disco duro o sistema operativo, la información tendrá un respaldo en el servidor. Este respaldo se puede hacer por medio de software para Backup o por mapeo de red desde el servidor. El tiempo de perdida en producción es muy bajo cuando procesos de backups funcionan correctamente, Ya que se tiene copias cifradas en disco y en la nube. En caso que se presente este inconveniente se podrá acceder a la información de forma remota y continuar con la producción.

* Activos de servicios: Servicios de autenticación de usuario y administración de procesos de usuario, enlaces, cortafuegos, servidores proxy, servicios de red, servicios inalámbricos, antispam, anti-virus, detección y/o prevención de intrusiones, seguridad, FTP, correo electrónico, mensajería instantánea, servicios web, contratos de soporte y mantenimiento de software.

|  |  |  |  |
| --- | --- | --- | --- |
| **Serial de la empresa** | **Serial externo** | **Nombre Equipo** | **Empresa** |
| SMN07 | XWOPRWX7 | Ubiquiti Unifi Uap-ac | SIMON |
| **Propietario** | **Grupo** | **Ubicación** | **Descripción** |
| SIMON | \SIMON | Medellín | UAP-AC-LR-US |
| **Dirección IP** | **Tipo** | **Fabricante** | **Serie** |
| 192.168.0.2 | Impresora | Ubiquiti Networks | UAP35A0F2H10 |
| **Deshabilitado** | **Origen** | **Fecha Activación** | **Fecha Modificación** |
| No | Manual | dd/mm/yyyy | dd/mm/yyyy |
| **Memoria** | **Capacidad de disco** | **Modelo CPU** | **Cargo** |
| - | - | - | Router WIFI |

|  |  |  |  |
| --- | --- | --- | --- |
| **Serial de la empresa** | **Serial externo** | **Nombre Equipo** | **Empresa** |
| SMN08 | XWPRWX8 | FORTINET 300D | SIMON |
| **Propietario** | **Grupo** | **Ubicación** | **Descripción** |
| SIMON | \SIMON | Medellín | 300D |
| **Dirección IP** | **Tipo** | **Fabricante** | **Serie** |
| 181.51.48.83 | Switch | FORTINET | FGT3HD3917801 |
| **Deshabilitado** | **Origen** | **Fecha Activación** | **Fecha Modificación** |
| No | Manual | dd/mm/yyyy | dd/mm/yyyy |
| **Memoria** | **Capacidad de disco** | **Modelo CPU** | **Cargo** |
| - | - | - | Firewall |

|  |  |  |  |
| --- | --- | --- | --- |
| **Serial de la empresa** | **Serial externo** | **Nombre Equipo** | **Empresa** |
| SMN09 | XWPRWX9 | QUIDWAY S2300 SERIES | SIMON |
| **Propietario** | **Grupo** | **Ubicación** | **Descripción** |
| SIMON | \SIMON | Medellín | S2318TP-EI |
| **Dirección IP** | **Tipo** | **Fabricante** | **Serie** |
| 181.51.48.85 | Switch | HUAWEI | CN6AGP50R9 |
| **Deshabilitado** | **Origen** | **Fecha Activación** | **Fecha Modificación** |
| No | Manual | dd/mm/yyyy | dd/mm/yyyy |
| **Memoria** | **Capacidad de disco** | **Modelo CPU** | **Cargo** |
| - | - | - | Ethernet |

Valoración de activos: Los activos de servicio juegan un papel importante en la organización. De ellos depende mucho la confiabilidad de la información. Es una combinación entre software y hardware que ayudan a la protección e integridad de la información. El firewall debe proteger la información de ataques de intrusos así como también el software de antivirus instalados en las maquinas. Un ataque que logre salta las barreras de seguridad puede causar daños en la información confidencial de la empresa. Las medidas de cifrado deben estar bien configuradas.

**Activos humanos**

* Empleados: personal, directivos, directores ejecutivos, arquitectos de software y desarrolladores, probadores, administradores de sistemas, administradores de seguridad, operadores, abogados, auditores, usuarios con poder y expertos en general
* Externos: trabajadores temporales, consultores externos o asesores especialistas, contratistas especializados, proveedores y socios.

Valoración de activos: Los activos humanos son fundamentales en el desenvolvimiento de las labores de la organización, son quienes llevan a cabo los procesos. Pero qué pasa si uno de estos activos no puede ir a laboral o tiene un accidente fatal y solo esta persona tenía el conocimiento o claves de acceso para poder llevar a cabo toda la producción en la empresa. Como medida de disponibilidad se debe tener manuales de procesos específicos y respaldo de llaves de seguridad. También realizar una valoración e inventario de las funciones que labora cada usuario un posible reemplazo en el menor tiempo.

**NORMATIVIDAD DE LA SEGURIDAD INFORMÁTICA**

La herramienta ISO-27001 para Riesgos y Seguridad de la Información, está capacitado para responder a numerosos controles para el tratamiento de la información gracias a las aplicaciones que contiene y que son totalmente configurables según los requerimientos de cada organización. Además, permite la automatización del Sistema de Gestión de Seguridad de la Información.

La norma ISO 27001:2013 se publicó el 25 de septiembre de 2013. La nueva ISO 27001:2013 trae cambios muy importantes, la estructura del estándar internacional ISO 27001 cambio al pasar de 8 cláusulas a 10, esto derivado de su alineación al Anexo SL. La norma ISO 27001 versión 2013 ya puede ser implantada en una organización. Con la nueva versión se aumentó el número de dominios de seguridad de 11 a 14. Los cambios que se realizan en el sector de la tecnología de la información son necesarios, sobre todo porque los servidores necesitan ser actualizados cada cierto tiempo.

**CONCLUSIÓN**

La disponibilidad hace referencia a que la información sea accesible y utilizable por el usuario a cargo de esta información o proceso. A partir de esto, las organizaciones deben desarrollar las estrategias y los instrumentos con los cuales los usuarios o propietarios puedan hacer uso de la información sin la menor interrupción posible.

La integridad hace referencia a la propiedad de salvaguardar la exactitud y estado completo de los activos. Para las organizaciones toda información es vital para funciones, procesos y procedimientos, por lo que la totalidad de esa información debe ser salvaguardada para cumplir con las funciones y procesos de la organización.

La confidencialidad hace referencia a la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

**BIBLIOGRAFÍA**

INCIBE, “Inventario de activos y gestión de la seguridad en SCI”. {En línea}. {Publicado el 29/12/2016} disponible en: (https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci).

Secretaria General, “Inventario de Activos de Información” {En línea}. (https://www.secretariageneral.gov.co/sites/default/files/linemientos-distritales/L\_11%20Inventario%20de%20Activos%20de%20Informaci%C3%B3n.pdf).

UNMSM, Plan de seguridad para una entidad financiera. {En línea}. http://sisbib.unmsm.edu.pe/bibvirtualdata/Tesis/Basic/Cordova\_RN/Cap4.pdf

Instituto Nacional de Ciber Seguridad de España, {En línea}. https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci