RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN ENTIDADES PÚBLICAS

Information security and privacy risks in public entities

Jose Yimy Arbey Gaona Reina
jganoa@ucundinamarca.edu.co
joseyimyarbey@gmail.com

Universidad de Cundinamarca, Facultad de Ingeniería, Programa de [sistemas]
Alcaldía de Fusagasugá, Oficina TIC, pasantía [ciberseguridad]

Resumen

En la actualidad es difícil e imposible, garantizar la seguridad al 100% de la información, debido a que el computador tiene acceso directo o indirecto al internet, y esta puede ser vulnerable. Debido a que acceder a la web se puede considerar una moneda del azar a veces puede ser fácil de manejar, un gran apoyo, y una excelente herramienta para el aprendizaje, en la búsqueda y recopilación de información, no obstante no deja de ser un peligro, para los datos e información personal, de un individuo o empresa, y puede ser filtrado un espía autorizado o no autorizado por el usuario, y esta puede robar, y usar de forma desagradable, o sin el conocimiento del usuario los datos e información (INFORMATICA, 2008). En la alcaldía municipal de Fusagasugá se dio apoyo para la mejora de su infraestructura y un punto esencial es la seguridad de sus datos, los cuales deben estar protegidos a cualquier amenaza, para esto fue primordial hacer un estudio de preservación de la información e implementación de la seguridad en dicha red. Donde se generaron protocolos de seguridad y desarrollo una política estricta para minimizar errores de filtración de los datos sensibles de la alcaldía municipal. Para garantizar que la información solo sea accedida por personas autorizadas teniendo como guía el Plan de Seguridad y Privacidad de la Información y Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Toda empresa se basa en la información para tomar decisiones que permitan la continuidad del negocio, transformándose así en un activo importante para las organizaciones, siendo necesario protegerla ante cualquier evento que puede causar corrupción en los datos. Dada la importancia de la información, organizaciones internacionales de estandarización han elaborado normas de buenas prácticas para el resguardo y buen uso de la información y de los activos en general.

A pesar de que la alcaldía municipal de Fusagasugá se mantiene estable en sus operaciones, nace la necesidad de empezar a gestionar controles de seguridad, para poder garantizar que la información no será alterada o manejada por personas no autorizadas y para poder mitigar esta necesidad. Por lo tanto, en las pasantías se tuvo como finalidad minimizar los riesgos de perdida, daño o alteración de la información dentro de la alcaldía municipal de Fusagasugá garantizando la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.

Palabras Clave: Activo de información: Cualquier información o sistema relacionado con el tratamiento de datos que tenga un valor para la organización. Amenaza: Circunstancia desfavorable que puede ocurrir de forma natural, accidental o intencionada y que deriva en un incidente de seguridad, Vulnerabilidad: Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota, Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Abstract

At present it is difficult and impossible to guarantee 100% security of the information, because the computer has direct or indirect access to the Internet, and this can be vulnerable. . Because accessing the web can be considered a currency of chance can sometimes be easy to handle, a great support, and an excellent tool for learning, in the search and collection of information, however it is still a danger, for the data and personal information, of an individual or company, and a spy authorized or not authorized by the user can be filtered, and this can steal, and use in an unpleasant way, or without the knowledge of the user the data and information (INFORMATICA, 2008). In the municipal mayor's office of Fusagasugá support was given for the improvement of its infrastructure and an essential point is the security of its data, which must be protected from any threat, for this it was essential to make a study of preservation of the information and implementation of security in said network. Where security protocols were generated and a strict policy was developed to minimize errors in the leakage of sensitive data of the municipal mayor's office. To ensure that the information is only accessed by authorized persons having as a guide the Information Security and Privacy Plan and the Information Security and Privacy Risk Treatment Plan. Every company relies on information to make decisions that allow business continuity, thus becoming an important asset for organizations, being necessary to protect it against any event that can cause corruption in data. Given the importance of information, international standardization organizations have developed standards of good practice for the safeguarding and proper use of information and assets in general. Although the municipal mayor's office of Fusagasugá remains stable in its operations, the need

to start managing security controls is born, in order to guarantee that the information will not be altered or handled by unauthorized persons and to be able to mitigate this need. Therefore, the purpose of the internships was to minimize the risks of loss, damage or alteration of information within the municipal mayor's office of Fusagasugá, guaranteeing the integrity and availability of information processing and communications services.

Keywords: Information asset: Any information or system related to data processing that has a value for the organization, hreat: Unfavorable circumstance that may occur naturally, accidentally or intentionally and that results in a security incident, or deficiencies in a program that can allow a non-legitimate user to access information or perform unauthorized operations remotely, Information Security: Preservation of the confidentiality, integrity and availability of information; in addition, other properties such as authenticity, liability, non-repudiation and reliability can also be considered.

1. INTRODUCCIÓN

La Información es parte de los activos más importantes de toda empresa, y a su vez es uno de los recursos más propenso a vulnerabilidades, siendo necesario protegerlo de amenazas internas y externas. En la actualidad las empresas necesitan que la información que manejan esté siempre disponible, sin alteraciones en sus datos y sea confiable. (BERMUDEZ KELLY, 2015). Para salvaguardar dicha información es fundamental implementar sistemas de gestión de seguridad, proporcionar un estándar de calidad de seguridad de la información, ayudando a que se mitiguen los riesgos de daños, robo fuga de información, permitiendo mantener la integridad, confidencialidad y disponibilidad de la información, y garantizar la autenticidad y el no repudio de la misma.

Es de gran importancia que se desarrollen estos protocolos y políticas ya que ayudan suplir las necesidades que se presentan en la misma. Para garantizar la confidencialidad, integridad y disponibilidad de la información. Mediante un arduo análisis de la seguridad informática y seguridad de información se podrán conocer estas vulnerabilidades y esto ayuda para aplicar controles de seguridad mediante el uso de protocolos y políticas para detener el acceso de personal no autorizado, garantizar la integridad y disponibilidad de los servicios procesamiento de información y comunicaciones, por lo tanto, se desea asegurar que los funcionarios, contratistas y terceros cumplan sus responsabilidades. Finalmente minimizar los riesgos de perdida, daño o alteración de la información dentro de la alcaldía municipal

1.1 Acontecimientos

Se En los últimos años las organizaciones se preocupan por sobre salir en los sistemas informáticos, en adaptarse al mundo de la tecnología, pero en la mayoría de los casos no le dan prioridad a la seguridad de la información. Cada día evoluciona más la tecnología y con ella las personas que descubrieron el valor de la información, donde buscan las vulnerabilidades de una empresa y la forma de robar la información sensible. ocasionándole daños perdidas monetarias y riesgos a las organizaciones. Hace un par de años, la compañía americana reconocía que, en 2013, fue víctima de un gran ataque informático que afectó a más de 1.000 datos personales de sus usuarios. Uno de sus grandes fallos fue, precisamente, haberse callado durante años, algo que provocó que su CEO fuera cesado de sus funciones.

La brecha de seguridad costó a Yahoo! unos 3.000 millones de dólares ya que se expusieron datos tan sensibles como direcciones de email, claves, cumpleaños, números de teléfonos, nombres y apellidos de las personas registradas en la plataforma. (APD, 2020) Actualmente es necesario garantizar que en los perfeccionamientos realizados en los sistemas informáticos y en la manipulación de la información física se incluyan criterios de seguridad de la información, pues está debe resguardarse y limitarse para evitar exponerla a personas ajenas a la utilización de la misma. Al no contar con unos protocolos previamente estudiados, se ven afectados por el hacking, el robo de la información y perdidas monetarias. Permite ver claramente como el uso adecuado de la seguridad puede subsanar estos errores que son fatales para una organización

En 2014, Sony vivió su particular annus horribilis con una serie de ciberataques a varias de sus divisiones que provocaron unas pérdidas millonarias a la compañía. Uno de esos ataques, mencionados por el propio Barack Obama como «intento de extorsión», fue el que afectó al departamento audiovisual.

Concretamente, los cibercriminales se dedicaron a robar correos y películas de la compañía, provocando la cancelación

de rodajes cinematográficos y, por ende, haciendo lo propio con los estrenos cinematográficos. Además de los ataques, se produjeron amenazas personales y, tras una larga investigación, el FBI responsabilizó de todos los incidentes a Corea del Norte.

A medida que la tecnología avanza el hacker negro lo hace también, donde siempre está en busca de romper la seguridad o buscar vulnerabilidades que le ayuden con su cometido. Todos estamos expuestos a estos ataques, lo esencial es generar conciencia y darles soporte el personal, generar capacitaciones para el buen uso de las tecnologías. Debemos proporcionar unas buenas políticas de seguridad, hacer constantemente pruebas y monitoreo de la red, para evaluar la integridad de los datos, almacenamiento, comunicación y servicios para verificar que no ocurra ninguna alteración de los datos sensibles.

Hace unos meses, el malware Wannacry se hacía tristemente famoso por haber sido capaz de infectar, a la vez, a cientos de multinacionales y organismos institucionales en todo el mundo. La española Telefónica fue una de sus víctimas y eso a pesar de contar entre sus filas con reputados profesionales de la seguridad IT, como es el caso de Chema Alonso.

Lo cierto es que la compañía actuó rápido y subsanó la exposición de datos de sus clientes, pero fue un claro ejemplo de que, por mucha vigilancia que haya, los cibercriminales siempre encuentran un hueco por el que escabullirse y hacer daño. Habiendo acreditado que la información forma parte de los activos más importantes dentro de una organización, es fundamental que en toda organización se generen controles de seguridad que les permita garantizar que la información contenida en sus sistemas informáticos sea confiable, siempre esté disponible y se mantenga íntegra, por lo cual incorporar lineamientos de seguridad en los procesos críticos de la empresa les permitirá minimizar posibles riesgos de fuga de información o el manejo incorrecto de la misma.

2. MATERIALES Y MÉTODOS/METODOLOGÍA

Modelo Integrado de Planeación y Gestión (MIPG)

Figura 1
Descripción del marco de referencia

Nota: Adaptado de "Modelo integrado de planeación y gestión", por función pública, mipg, 2017.

MIPG es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, según dispone el Decreto1499 de 2017. Ver Figura 1 Es un marco de referencia porque contempla un conjunto de conceptos, elementos, criterios, que permiten llevar a cabo la gestión de las entidades públicas. Enmarca la gestión en la calidad y la integridad, al buscar su mejoramiento permanentemente para garantizar los derechos, satisfacer las necesidades y expectativas de la ciudadanía.

El fin de la gestión es generar resultados con valores, es decir, bienes y servicios que tengan efecto en el mejoramiento del bienestar de los ciudadanos, obtenidos en el marco de los valores del servicio público (Honestidad, Respeto, Compromiso,

Diligencia y Justicia).
Busca generar valor público a través de la entregan resultados que respondan y satisfagan las necesidades y demandas de los ciudadanos. (DESEMPEÑO, 2018)

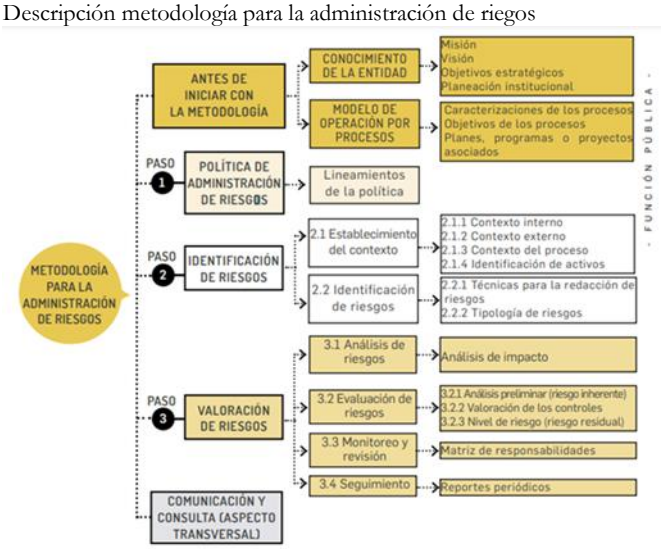
ISO 27001

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.
El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).
Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.
ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

SGSI

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de políticas de administración de la información. El término se denomina en inglés "Information Security Management System" (ISMS).
El término SGSI es utilizado principalmente por la ISO/IEC 27001, que es un estándar internacional aprobado en octubre de 2005 por la International Organization for Standardization y por la comisión International Electrotechnical Commission.
La ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming": PDCA – acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar), siendo éste un enfoque de mejora continua:
•Plan (planificar): es una fase de diseño del SGSI de evaluación de riesgos de seguridad de la información y la selección de controles adecuados.
•Do (hacer): es una fase que envuelve la implantación y operación de los controles.
•Check (controlar): es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
•Act (actuar): en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.
El concepto clave de un SGSI es el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información, ver Figura 2.
Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización, así como los externos del entorno. (wikipedia, 2020)

Figura 2
Descripción metodología para la administración de riegos



Nota: Adaptado de "Sistema de Gestión de la Seguridad de la Información", por función pública, M.D, 2018.

Modelo De Gestión De Riesgos De Seguridad Digital (MGRSD)

El objetivo principal de este anexo es orientar a todas las entidades del Gobierno nacional, territoriales y sector público en la implementación de la gestión de riesgos de seguridad digital basada en la definición metodológica del MGRSD para, entre otros aspectos, incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en cada entidad pública. (INFORMACIÓN, 2018)

3. RESULTADOS Y DISCUSIÓN

"La realización de un inventario y clasificación de activos hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información con respecto a la seguridad de los activos de información de los procesos de una entidad" teniendo como guía el Modelo de Seguridad y Privacidad de la Información se da como objetivo dar cumplimiento a los cuatro puntos principales inventario de activos, propiedad de los activos, clasificación de la información, etiquetado y manipulación de la información siguiendo Controles del estándar ISO/IEC 27001:2013.

De este modo se identifica los activos de información teniendo en cuenta tipo de activo según la Clasificación estructurada, teniendo como guía el Plan de Seguridad y Privacidad de la Información y Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. Ver Tabla 1

Tabla 1

Cronograma dado por la oficina para la recolección del inventario de activos, por dependencia semana y mes.

	DEPENDENCIA	Mes 1				Mes 2	
		SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2
	DESPACHO ALCALDE						
1.1.	Oficina de Desarrollo Institucional						
1.2.	Oficina de Control Interno						
1.3.	Oficina de Control Interno Disciplinario						
1.4.	Oficina de Turismo						
1.5.	Oficina de Proyectos						
1.6.	Oficina TIC						
1.7.	Oficina Asesora de Comunicaciones						
1.8.	Oficina de Solidaridad						
	SECRETARÍA JURÍDICA						
2.1.	Dirección de Defensa Judicial y Asuntos Jurídicos						
2.2.	Dirección de Contratación						
	SECRETARÍA DE GOBIERNO, SEGURIDAD Y CONVIVENCIA						
	3.0. 1. Áreas de Trabajo de Corregimiento						
3.1.	Dirección de Participación y Asuntos Locales						
3.1.1.	Área de Trabajo de Comisarias de Familia						
3.2	Dirección de Seguridad y Convivencia Ciudadana						
3.2.1.	Área de Trabajo de Inspecciones de Policía						
3.2.2.	Área de Trabajo de Protección al Consumidor y Establecimientos Comerciales						
	SECRETARÍA DE EDUCACIÓN						
4.1.	Dirección del Servicio Educativo						
	4.1.1 Área de Trabajo de Calidad Educativa						
4.1.2.	Área de Trabajo de Cobertura Educativa						
4.1.3.	Área de Trabajo Administrativa y Financiera						
	SECRETARÍA DE PLANEACIÓN						

Nota: El cronograma se efectúa en su totalidad Adaptado de "cronograma inventario equipo de red", por Ivon, 2021.

teniendo como guía el cronograma se recolecta la información de activos y se llena el formato dado con la oficina tic que permite clasificar los activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un proceso.

Figura 3

Descripción clasificación de activos revisión, actualización, definición y publicación.

Nota: Adaptado de "Activos de información", por función pública, , 2018.

Al momento de generar la clasificación se tiene en cuenta

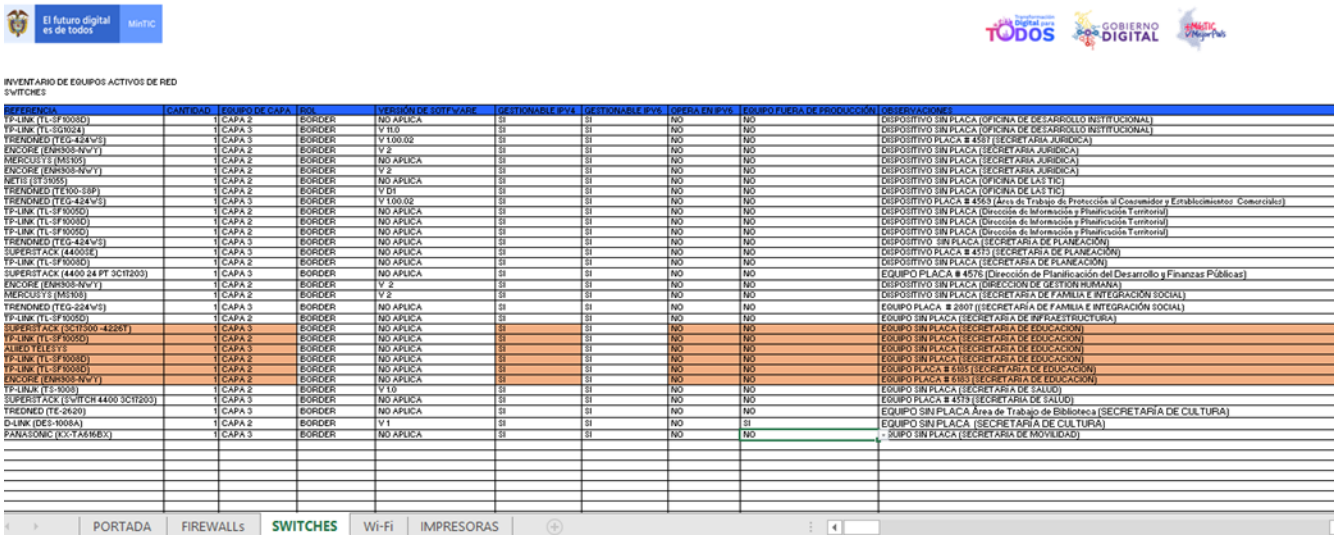
CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN.

La clasificación de activos de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados, ya que con base en su valor y de acuerdo a otras características particulares requiere un tipo de manejo especial. Ver Figura 3 El sistema de clasificación de la información que podría definirse en la entidad se basa las características particulares de la información, contempla la cultura y el funcionamiento interno y buscando dar cumplimiento a los requerimientos estipulados en el ítem relacionado con la Gestión de Activos de los estándares 27001:2013, ISO 27002, e ISO 27005.

Como medida necesaria se tiene en cuenta la guía para generar la documentación de recolección de activos, Ver Tabla 2

Tabla 2

Activos de red de switches, puntos wifi, impresoras, firewall.



INVENTARIO DE EQUIPOS ACTIVOS DE RED
SWITCHES

REFERENCIA	CANTIDAD	EQUIPO DE CAPA	ROL	VERSIÓN DE SOTFWARE	GESTIONABLE IPV4	GESTIONABLE IPV6	OPERA EN IPV6	EQUIPO FUERA DE PRODUCCIÓN	OBSERVACIONES
TP-LINK (TL-SF1008D)	1	CAPA 2	BORDER	NO APLICA	SI	SI	NO	NO	DISPOSITIVO SIN PLACA (OFICINA DE DESARROLLO INSTITUCIONAL)
TP-LINK (TL-SG1024)	1	CAPA 2	BORDER	V 11.0	SI	SI	NO	NO	DISPOSITIVO SIN PLACA (OFICINA DE DESARROLLO INSTITUCIONAL)
TRENDNED (TEG-424WS)	1	CAPA 3	BORDER	V 1.00.02	SI	SI	NO	NO	DISPOSITIVO PLACA # 4587 (SECRETARIA JURIDICA)
ENCORE (ENH308-NWY)	1	CAPA 2	BORDER	V 2	SI	SI	NO	NO	DISPOSITIVO SIN PLACA (SECRETARIA JURIDICA)
MERCUSYS (MS105)	1	CAPA 2	BORDER	NO APLICA	SI	SI	NO	NO	DISPOSITIVO SIN PLACA (SECRETARIA JURIDICA)
ENCORE (ENH308-NWY)	1	CAPA 2	BORDER	V 2	SI	SI	NO	NO	DISPOSITIVO SIN PLACA (SECRETARIA JURIDICA)
NETIS (ST31055)	1	CAPA 2	BORDER	NO APLICA	SI	SI	NO	NO	DISPOSITIVO SIN PLACA (OFICINA DE LAS TIC)
TRENDNED (TE100-S8P)	1	CAPA 2	BORDER	V D1	SI	SI	NO	NO	DISPOSITIVO SIN PLACA (OFICINA DE LAS TIC)
TRENDNED (TEG-424WS)	1	CAPA 3	BORDER	V 1.00.02	SI	SI	NO	NO	DISPOSITIVO PLACA # 4563 (Área de Trabajo de Protección al Consumidor y Establecimientos Comerciales)
TP-LINK (TL-SF1005D)	1	CAPA 2	BORDER	NO APLICA	SI	SI	NO	NO	DISPOSITIVO SIN PLACA (Dirección de Información y Planificación Territorial)
TP-LINK (TL-SF1008D)	1	CAPA 2	BORDER	NO APLICA	SI	SI	NO	NO	DISPOSITIVO SIN PLACA (Dirección de Información y Planificación Territorial)
TP-LINK (TL-SF1005D)	1	CAPA 2	BORDER	NO APLICA	SI	SI	NO	NO	DISPOSITIVO SIN PLACA (Dirección de Información y Planificación Territorial)
TRENDNED (TEG-424WS)	1	CAPA 3	BORDER	NO APLICA	SI	SI	NO	NO	DISPOSITIVO SIN PLACA (SECRETARIA DE PLANEACIÓN)
SUPERSTACK (44005E)	1	CAPA 3	BORDER	NO APLICA	SI	SI	NO	NO	DISPOSITIVO PLACA # 4573 (SECRETARIA DE PLANEACIÓN)
TP-LINK (TL-SF1008D)	1	CAPA 2	BORDER	NO APLICA	SI	SI	NO	NO	DISPOSITIVO SIN PLACA (SECRETARIA DE PLANEACIÓN)
SUPERSTACK (4400 24 PT 3C17203)	1	CAPA 3	BORDER	NO APLICA	SI	SI	NO	NO	EQUIPO PLACA # 4576 (Dirección de Planificación del Desarrollo y Finanzas Públicas)
ENCORE (ENH308-NWY)	1	CAPA 2	BORDER	V 2	SI	SI	NO	NO	DISPOSITIVO SIN PLACA (DIRECCION DE GESTION HUMANA)
MERCUSYS (MS108)	1	CAPA 2	BORDER	V 2	SI	SI	NO	NO	DISPOSITIVO SIN PLACA (SECRETARIA DE FAMILIA E INTEGRACIÓN SOCIAL)
TRENDNED (TEG-224WS)	1	CAPA 3	BORDER	NO APLICA	SI	SI	NO	NO	EQUIPO PLACA # 2807 ((SECRETARÍA DE FAMILIA E INTEGRACIÓN SOCIAL)
TP-LINK (TL-SF1005D)	1	CAPA 2	BORDER	NO APLICA	SI	SI	NO	NO	EQUIPO SIN PLACA (SECRETARIA DE INFRAESTRUCTURA)
SUPERSTACK (3C17300 -4226T)	1	CAPA 3	BORDER	NO APLICA	SI	SI	NO	NO	EQUIPO SIN PLACA (SECRETARIA DE EDUCACION)
TP-LINK (TL-SF1005D)	1	CAPA 2	BORDER	NO APLICA	SI	SI	NO	NO	EQUIPO SIN PLACA (SECRETARIA DE EDUCACION)
ALIED TELESYS	1	CAPA 3	BORDER	NO APLICA	SI	SI	NO	NO	EQUIPO SIN PLACA (SECRETARIA DE EDUCACION)
TP-LINK (TL-SF1008D)	1	CAPA 2	BORDER	NO APLICA	SI	SI	NO	NO	EQUIPO SIN PLACA (SECRETARIA DE EDUCACION)
TP-LINK (TL-SF1008D)	1	CAPA 2	BORDER	NO APLICA	SI	SI	NO	NO	EQUIPO PLACA # 6185 (SECRETARIA DE EDUCACION)
ENCORE (ENH308-NWY)	1	CAPA 2	BORDER	NO APLICA	SI	SI	NO	NO	EQUIPO PLACA # 6183 (SECRETARIA DE EDUCACION)
TP-LINJK (TS-1005)	1	CAPA 2	BORDER	V 1.0	SI	SI	NO	NO	EQUIPO SIN PLACA (SECRETARIA DE SALUD)
SUPERSTACK (SWITCH 4400 3C17203)	1	CAPA 3	BORDER	NO APLICA	SI	SI	NO	NO	EQUIPO PLACA # 4573 (SECRETARIA DE SALUD)
TRENDNED (TE-2620)	1	CAPA 3	BORDER	NO APLICA	SI	SI	NO	NO	EQUIPO SIN PLACA Área de Trabajo de Biblioteca (SECRETARÍA DE CULTURA)
D-LINK (DES-1008A)	1	CAPA 2	BORDER	V 1	SI	SI	NO	SI	EQUIPO SIN PLACA (SECRETARÍA DE CULTURA)
PANASONIC (KX-TA616BX)	1	CAPA 3	BORDER	NO APLICA	SI	SI	NO	NO	- EQUIPO SIN PLACA (SECRETARIA DE MOVILIDAD)

PORTADA | FIREWALLS | SWITCHES | Wi-Fi | IMPRESORAS

Nota: Se completa la recolección de activos Adaptado de "Activos de red entidades publicas", por función Mintic, 2020.

"La Información es parte de los activos más importantes de toda empresa, y a su vez es uno de los recursos más propenso a vulnerabilidades, siendo necesario protegerlo de amenazas internas y externas. En la actualidad las empresas necesitan que la información que manejan esté siempre disponible, sin alteraciones en sus datos y sea confiable". (BERMUDEZ KELLY, 2015) Para salvaguardar dicha información es fundamental implementar el Modelo De Gestión De Riesgos De Seguridad Digital (MGRSD), proporcionar un estándar de calidad de seguridad de la información, ayudando a que se mitiguen los riesgos de daños, robo fuga de información, permitiendo mantener la integridad, disponibilidad de la información, confidencialidad, garantizar la autenticidad y el no repudio de la misma.

Por tal motivo en esta actividad teniendo como base el Modelo De Gestión De Riesgos De Seguridad Digital (MGRSD) se procede a salvaguardar la información para que esta se mantenga con integridad disponibilidad y confidencialidad, generando un manual el cual ayuda a sistematizar la información de cada funcionario y lograr mantener la información integral, este manual Ver Figura 5 cuenta con un paso a paso, para que el usuario por medio de la red y permisos de administrador, pueda almacenar la información sensible y poder controlar posibles amenazas y riesgos cibernéticos.

Figura 5

Descripción de la tabla de contenido del manual MGRSD qnap.

Tabla de contenido

Nota: Adaptado de "Manual MGRSD qnap", por Yimy Gaona & Carlos Abril, 2021

4. CONCLUSIONES

- De acuerdo con lo anterior, se puede aseverar que se desarrolló continuamente procesos de identificación y clasificación de riesgos de seguridad y hacer un estudio de la infraestructura y estimar los activos de información teniendo en cuenta tipo de activo según la Clasificación estructurada por el Área de Seguridad. Y cómo solventar estos riesgos para garantizar la confidencialidad, integridad y disponibilidad de la información, siguiendo una serie de funciones y lineamientos de acuerdo con la guía para la administración del riesgo y el diseño de controles en entidades públicas.
- Finalmente se logra determinar que los lineamientos para la gestión de riesgos de seguridad digital en entidades públicas si logra garantizan la integridad y disponibilidad de los servicios de procesos de información, pero esta debe actualizarse en periodos cortos para mitigar nuevas amenazas que se vayan presentando.

REFERENCIAS

ADP, «ADP,» 2020. [En línea]. Available: https://www.apd.es/empresas-afectadas-por-ciberataques/.

B. KELLY, «UNIVERSIDAD POLITECNICA,» MARZO 2015. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf.

D. e. imagen, «Dinero en imagen,» 2021. [En línea]. Available: https://www.dineroenimagen.com/hacker/62-terminos-que-tienes-que-conocer-para-mejorar-tu-seguridad-informatica/100039.

DESEMPEÑO, «MINTIC,» OCTUBRE 2018. [En línea]. Available: https://www.mincit.gov.co/ministerio/planeacion/modelo-integrado-de-planeacion-y-gestion/manual-operativo-mipg-v2-oct-2018.aspx.

ERIC, «FUNDAMENTOS DE SEGURIDAD- MEXICO,» 19 ENERO 2018. [En línea]. Available:

https://gsitic.wordpress.com/2018/01/19/bii13-seguridad-fisica-y-logica-de-un-sistema-de-informacion-riesgos-amenazas-y-vulnerabilidades-medidas-de-proteccion-y-aseguramiento-auditoria-de-seguridad-fisica/#:~:text=La%20seguridad%20f%C3%ADsica%20trata%20de.

INFORMACION, «FUNCION PUBLICA,» 2018. [En línea]. Available: https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657.

INFORMATICA, «SEGURIDAD WEB,» JUNIO 2008. [En línea]. Available: http://seguridadinformatica2008.blogspot.com/2008/06/planteamiento-del-problema.html.

MINTIC. (2016). *Sguridad y Pivacidad De La Información. Obtenido de Guía para la Gestión y Clasificación: https://mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf*

WIKIPEDIA, «WIKIPEDIA,» 29 SEPTIEMBRE 2020. [En línea]. Available: https://es.wikipedia.org/wiki/ISO/IEC_27001WI.