ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DEFINICIÓN DEL PROCESO DE CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN PARA EL CENTRO DE OPERACIONES DE SEGURIDAD INFORMÁTICA SECUINFOR S.A."

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

MICHELLE IVETTE PRENDES MORENO

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTO

Mis sinceros agradecimientos a Christian Mendoza y Karina Astudillo por el apoyo logístico y en conocimientos para llevar a cabo el presente trabajo. A Christian Vargas por su desinteresada ayuda para completar esta etapa. Y a mis amigos: Andrea Quintero, Wendy Vera, Geovanny Valle, Manuel Banchón, Mauricio Torres, Mayra Espín, John Palomeque, Oswaldo García, Enrique Rodas, Gonzalo Argudo, Gustavo Mazzini y Yolanda Moreta, por el seguimiento y sobre todo por el aliento. Finalmente quiero agradecer a Sean, mi compañero de vida, por estar presente cada día, por el amor y el apoyo infinito para la realización de mis proyectos. ¡Gracias!

DEDICATORIA

El presente proyecto lo dedico a Dios, a mi padre, Johnny Prendes; a mi madre, Narcisa Moreno; a mis hermanas, Lissette y Samantha; a mi cuñado, Emilio Ramirez y a mi amor pequeño, mi sobrina, Emma, por el infinito amor, soporte y empuje no solo en este proyecto sino también a lo largo de mi vida.

TRIBUNAL DE SUSTENTACIÓN

MGS. Lenin Freire C.	**MGS. Juan Carlos García P.**
EVALUADOR	EVALUADOR

RESUMEN

SECUINFOR S.A. maneja información sensible tanto propia como de sus clientes. Por ello la clasificación de sus activos de información es una necesidad imperante para poder ejercer los controles y tratamientos adecuados de la misma. Al momento, la inexistencia de esta clasificación, dificulta la toma de decisiones estratégicas de esta empresa. Adicionalmente, disponer de un proceso de clasificación de sus activos de información sería el arranque para la preparación para certificarse en ISO 27001, que es otro de los proyectos de SECUINFOR S.A. El desarrollo de este proceso consistió en el uso de estándares internacionales como guías de trabajo, la identificación de la información, en función de su relevancia y uso en la empresa y la categorización de la información y definición de los criterios de clasificación basado en los principios de seguridad como confidencialidad, integridad y disponibilidad. Finalmente se aplicó, a manera de piloto, el proceso desarrollado a una muestra de datos del sistema de información del servicio de Respaldo en Nube.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

SECUINFOR S.A., como empresa de seguridad informática, tiene la necesidad imperante de contar con un proceso de clasificación de los activos de información que maneja y posee. Este proyecto tiene como objetivo definir el proceso de clasificación de los activos de información para SECUINFOR S.A. apoyado en los estándares FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems [1], Volume I and II: Guide for Mapping Types of Information and Information Systems to Security Categories [2] [3], NYS ITS IT Standard: Information Classification [4] y Guidelines for Data Classification de la Universidad de Carnegie Mellon [5].

Se expone en este trabajo las bases tomada de los estándares, el diseño propuesto de proceso de clasificación y una prueba piloto aplicando el proceso resultante a dos muestras de activo de información escogida por SECUINFOR S.A.

CAPÍTULO 1

GENERALIDADES

SECUINFOR S.A. es una empresa cuyo núcleo de negocio es el ofrecimiento de servicios de seguridad informática; específicamente es un centro de operaciones de seguridad. Debido a sus operaciones, manejan información sensible propia como de sus clientes.

El objetivo de este proyecto es definir un proceso que permita clasificar los activos de información que posee y maneja la empresa. Para fines de este documento, se aplican las siguientes definiciones:

Activo de información: cualquier dato o información que tenga valor para la empresa y que puede ser creada, contenida, tratada o eliminada en cualquier formato -electrónico o no- por cualquier sistema de información propio, ajeno o relacionado a la organización. [6]

Confidencialidad: objetivo de seguridad que garantiza que la información sea revelada únicamente a personal o sistema autorizado.

Disponibilidad: objetivo de seguridad que garantiza que la información es accesible y utilizable por personal o sistema autorizado en cualquier momento.

Integridad: objetivo de seguridad que garantiza que la información este completa, no sea alterada o destruida por personal o sistema no autorizado.

Proceso: conjunto de tareas y/o procedimientos que dan tratamiento a una entrada usando diferentes recursos, los cuales puedes ser personas o sistemas, para generar una salida. Las entradas y salidas de un proceso pueden ser salidas y entradas de otros.

Sistema de Información: Sistema cuyos componentes tienen como función el tratamiento, procesamiento y gestión de la información para su posterior uso.

Categorización de Seguridad: asignación de un nivel de impacto por objetivo de seguridad (Confidencialidad, Integridad, Disponibilidad) a un tipo de información o sistema de información.

Clasificación de Información: determinación del nivel de exposición (Publica, Privada, Restringida) de una información hacia adentro y/o hacia afuera de una empresa.

1.1 Descripción del problema

Debido a la sensibilidad de la información que SECUINFOR S.A. maneja, se vuelve imperante su clasificación para poder ejercer los controles y tratamientos

adecuados de la misma. Por otro lado, esta clasificación de activos de información en función de las necesidades y aspectos críticos del negocio, facilitaría de gran manera la toma de decisiones estratégicas de la empresa, que al momento se encuentra limitada debido a su inexistencia.

Adicionalmente, contar con un proceso de clasificación de activos de información definido permitirá dar inicio a la preparación para la certificación ISO 27001, que es el proyecto que SECUINFOR S.A. se ha propuesto lograr a mediano plazo, en su afán de ser competitiva y ofrecer servicio de la mejor calidad a sus clientes.

1.2 Objetivo y Alcance

El proyecto presente tiene como objetivo principal definir un proceso que permita categorizar y clasificar la información que tenga valor para la empresa (activos de información). Este proceso definido será aplicable a la empresa y ajustado a sus necesidades. La definición de cualquier proceso adicional que sirva de entrada o sea salida del presente proceso en definición, está fuera del alcance de este proyecto.

1.3 Solución Propuesta

Se propone la definición de un proceso que permita categorizar y clasificar los activos de información de la empresa. El desarrollo de este proceso consistirá en:

- El uso de estándares internacionales como guías de trabajo: Esto asegurará que el proceso final esté basado en las buenas prácticas comprobadas internacionalmente

- Recolección de información identificada en función de su relevancia y uso en la empresa.
- La definición de los criterios de clasificación de la información: se la efectuará acorde a los principios de seguridad como confidencialidad, integridad y disponibilidad, los cuales permitirán un enfoque óptimo de seguridad de la información para la organización.

CAPÍTULO 2

METODOLOGÍA DEL DESARROLLO DE LA SOLUCIÓN

La metodología para el desarrollo de la solución propuesta consiste en cuatro etapas: la búsqueda y elección de estándares internacionales para la clasificación de información, la identificación de la información en función de la actividad o actividades núcleo de la empresa, la definición de los criterios a utilizarse para la clasificación de la información para finalmente definir los pasos del proceso de clasificación de activos de información.

2.1 Consulta de estándares de clasificación de la información

Se buscaron estándares para la clasificación de la información en Internet y se hallaron los siguientes:

- FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems (Estándar para la Categorización de la Información y Sistemas de Información Federales). Desarrollado por el Instituto Nacional de Estándares de Tecnología de los Estados Unidos de América NIST.

- SP800-60 Volume I y II: Guide for Mapping Types of Information and Information Systems to Security Categories (Guía para mapear tipos de Información y Sistema de Información en Categorías de Seguridad). Desarrollo por el Instituto Nacional de Estándares de Tecnología de los Estados Unidos de América.

- IT Standard: Information Classification (Estándar TI: Clasificación de la Información). Elaborado por la Oficina de Servicios de Tecnología de la Información del Estado de Nueva York.

- Guidelines for Data Classification (Directrices para la Clasificación de los datos) de la Universidad de Carnegie Mellon.

- Data Classification and Security Policy (Políticas de Seguridad y Clasificación de los datos) de la Universidad del Estado de Kansas.

De estos tres estándares y guías se decidió trabajar con los dos primeros debido a la consideración de las categorías de seguridad detalladas en ellos, por su generalidad que permitía una mejor adaptación al tipo de empresa tratada en este proyecto y por su aplicación probada ya en un país que da alta importancia a la seguridad de la información; y con el tercero, por ser una guía de sencilla

comprensión para la clasificación final de la información y por seguir categorizaciones congruentes con los dos primeros estándares.

2.1.1 Objetivos de Seguridad y Niveles de Impacto

De estos estándares se extraen las siguientes recomendaciones de métodos:

Deben establecerse la categorización de la información en función de los objetivos de seguridad y del nivel de impacto que tendría la afectación de la información desde el punto de vista de cada uno de los objetivos de seguridad, que en adelante llamaremos criterios.

El impacto se basa en las consecuencias de afectación al negocio, sean estas:

- Incapacidad de operar
- Pérdidas financieras
- Daño a los activos de la organización
- Daños intangibles como afectación a la reputación del negocio.

Las anteriores son referencias de impacto para el negocio y estableciendo un valor para los niveles de impacto tenemos una matriz que nos ayudaría a categorizar la información.

Así, tomaremos las definiciones de objetivos de seguridad y niveles de impacto establecidos en FIPS PUBS 199. Se exponen los mismos en las tablas 1 y 2 [2], cuya fuente de información es el estándar nombrado:

Tabla 1: Objetivos de Seguridad.

Objetivos de seguridad	Definición de FIPS 199
Confidencialidad	Pérdida de Confidencialidad es la revelación no autorizada de la información
Integridad	Pérdida de la Integridad es la modificación o destrucción no autorizada de la información
Disponibilidad	Pérdida de la Disponibilidad es la interrupción del acceso a o uso de la información

Tabla 2: Nivel de Impacto Potencial

Nivel de Impacto Potencial	Definición
Bajo	Cuando la pérdida de alguno de los criterios de seguridad puede ocasionar un efecto adverso limitado en las operaciones y activos organizacionales: Un efecto limitado significa que la pérdida de la confidencialidad, integridad o disponibilidad podría: (i) causar degradación en la capacidad de operación en una duración en la que la organización aún puede realizar sus funciones primarias, pero la efectividad de las funciones es reducida (ii) resultar en daño menor a los activos de la organización (iii) resultar en una pérdida financiera menor. (iv) resultar en daño menor a los individuos
Moderado	Cuando la pérdida de alguno de los criterios de seguridad puede ocasionar un efecto adverso serio en las operaciones y activos organizacionales: Un efecto serio significa que la pérdida de la confidencialidad, integridad o disponibilidad podría: (i) causar degradación significativa en la capacidad de operación en una duración en la que la organización aún puede realizar sus funciones primarias, pero la efectividad de las funciones es significativamente reducida (ii) resultar en daño significativo a los activos de la organización (iii) resultar en una pérdida financiera significativa. (iv) resultar en daño significativo sin muerte o heridas de muerte a la vida de los individuos
Alto	Cuando la pérdida de alguno de los criterios de seguridad puede ocasionar un efecto adverso severo o catastrófico en las operaciones y activos organizacionales: Un efecto severo o catastrófico significa que la pérdida de la confidencialidad, integridad o disponibilidad podría: (i) causar degradación severa en la capacidad de operación en una duración en la que la organización no puede realizar una o más de sus operaciones primarias (ii) resultar en daño mayor a los activos de la organización (iii) resultar en una pérdida financiera significativa. (iv) resulta en daño catastrófico o perdida de vida o heridas de muerte a los individuos

Una vez establecidos los criterios e impactos se define entonces una matriz en la que se categorizarían la información:

Tabla 3: Niveles de Impacto por Objetivo de Seguridad

	NIVEL DE IMPACTO		
OBJETIVO DE SEGURIDAD	**BAJO**	**MODERADO**	**ALTO**
Confidencialidad Preservar las restricciones autorizadas y el acceso y revelación de la información incluyendo los medios de la protección de la privacidad personal e información propietaria	La revelación no autorizada de la información podría causar un efecto adverso **limitado** a las operaciones y activos de la organización y a las personas	La revelación no autorizada de la información podría causar un efecto adverso **serio** a las operaciones y activos de la organización y a las personas	La revelación no autorizada de la información podría causar un efecto adverso **severo o catastrófico** a las operaciones y activos de la organización y a las personas
Integridad Guardar en contra de la modificación o destrucción inapropiada e incluye asegurar la autenticidad y el no repudio de la información	La modificación o destrucción no autorizada de la información podría causar un efecto adverso **limitado** a las operaciones y activos de la organización y a las personas	La modificación o destrucción no autorizada de la información podría causar un efecto adverso **serio** a las operaciones y activos de la organización y a las personas	La modificación o destrucción no autorizada de la información podría causar un efecto adverso **severo o catastrófico** a las operaciones y activos de la organización y a las personas
Disponibilidad Asegurar el uso y acceso confiable y a tiempo de la información	La interrupción del acceso o uso de la información o un sistema de información podría causar un efecto adverso **limitado** a las operaciones y activos de la organización y a las personas	La interrupción del acceso o uso de la información o un sistema de información podría causar un efecto adverso **serio** a las operaciones y activos de la organización y a las personas	La interrupción del acceso o uso de la información o un sistema de información podría causar un efecto adverso **severo o catastrófico** a las operaciones y activos de la organización y a las personas

Entonces, para cada tipo de información o sistema de información se tendrá la siguiente Categorización de Seguridad (SC por sus siglas correspondientes a Security Category) [1]:

$SC_{\text{tipo de información}}$ = {(confidencialidad, impacto), (integridad, impacto), (disponibilidad, impacto)} (2.1)

Más adelante, aplicaremos esta función cuando definamos los tipos de información de la empresa.

2.1.2 Proceso de Categorización de Seguridad

El siguiente paso es el proceso general que sigue el mapeo de la información. Para el efecto necesitamos contar con los sistemas de información de la organización definidos ya que esta es la entrada del proceso:

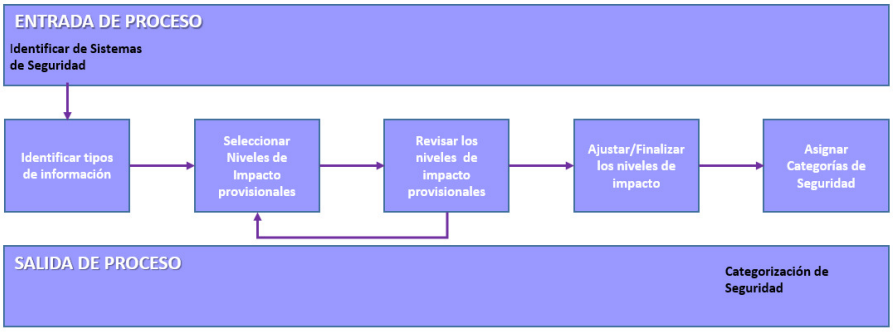


Figura 2.1: Proceso de Categorización de Seguridad

Según este proceso [1] debemos tener ya identificados los sistemas de información de la empresa, El siguiente paso sería identificar los tipos de información dentro del sistema de información analizado. Se procede luego a asignar un nivel de impacto provisional que luego será revisado y ajustado. Al quedar el nivel de impacto final, se tiene como resultado la

categorización de seguridad del sistema de información y del tipo de información.

Para obtener la Categoría de Seguridad (SC) de un sistema de información, se deben comparar los niveles de impacto de cada uno de los objetivos de seguridad de las SC de los tipos de información que contiene. Entonces, el nivel de impacto de cada objetivo de seguridad del sistema de información siempre será el valor más alto de impacto respecto al objetivo de seguridad de entre los tipos de información que el sistema posee [1]. Por ejemplo, para un sistema de información que contenga el tipo de información 1 y el tipo de información 2 se tendrá que, si las categorías de seguridad para los tipos de información son:

$SC_{\text{tipo de información 1}}$ = {(confidencialidad, BAJO), (integridad, BAJO), (disponibilidad, ALTO)} (2.2)

$SC_{\text{tipo de información 2}}$ = {(confidencialidad, BAJO), (integridad, MODERADO), (disponibilidad, MODERADO)} (2.3)

La categoría de seguridad para el sistema de información que contiene esos tipos de información se obtendrá comparando cada nivel de impacto con su objetivo de seguridad. Comparo entonces:

Para la confidencialidad, el nivel de impacto para el tipo de información 1 es BAJO y para el tipo de información 2 es BAJO. Por tanto, para el sistema de información, el impacto de la confidencialidad es BAJO.

Para la integridad, el nivel de impacto para el tipo de información 1 es BAJO y para el tipo de información 2 es MODERADO. Por tanto, para el sistema de información, el impacto de la integridad es MODERADO.

Para la disponibilidad, el nivel de impacto para el tipo de información 1 es ALTO y para el tipo de información 2 es MODERADO. Por tanto, para el sistema de información, el impacto de la disponibilidad es ALTO.

De esta forma la categoría de seguridad del sistema de información nos queda como:

$SC_{\text{sistema de información}}$ = {(confidencialidad, BAJO), (integridad, MODERADO), (disponibilidad, ALTO)} (2.4)

2.1.3 Identificación de los Tipos de Información

La identificación de los tipos de información mostrada en el Volumen I del Mapeo de los tipos de información y sistemas de información a Categorías de Seguridad [2] [3], consiste básicamente en la identificación de las actividades principales de la organización (definidas en la guía como):

- de propósito,
- de mecanismos que sirvan al propósito,
- de soporte a las operaciones,
- de funciones administrativas.

Los tipos de información que caigan en las primeras dos clases de actividades serán considerados Tipos de Información de Misión de la

empresa. Y los tipos de información que caigan en las dos siguientes actividades serán considerados Tipos de Información de Servicio.

Esta es una consideración hecha para entidades gubernamentales. Esta guía muestra entonces tablas de tipos de información mapeados a sus sistemas de información de acuerdo a las actividades principales de la organización. A continuación, una de las tablas mapeadas.

Table 4: Mission-Based Information Types and Delivery Mechanisms[14]

Services Delivery Mechanisms and Information Types [Mode of Delivery]		
D.20 Knowledge Creation & Management	**D.22 Public Goods Creation & Management**	**D.24 Credit and Insurance**
Research and Development	Manufacturing	Direct Loans
General Purpose Data and Statistics	Construction	Loan Guarantees
Advising and Consulting	Public Resources, Facility and Infrastructure Management	General Insurance
Knowledge Dissemination	Information Infrastructure Management	**D.25 Transfers to State/ Local Governments**
D.21 Regulatory Compliance & Enforcement	**D.23 Federal Financial Assistance**	Formula Grants
Inspections and Auditing	Federal Grants (Non-State)	Project/Competitive Grants
Standards Setting/Reporting Guideline Development	Direct Transfers to Individuals	Earmarked Grants
Permits and Licensing	Subsidies	State Loans
	Tax Credits	**D.26 Direct Services for Citizens**
		Military Operations
		Civilian Operations

Figura 2.2: Tipos de Información mapeados a Información basada en Misión

El estándar FIPS PUB 199 de NIST, indica que cada agencia (del gobierno) debe identificar sus tipos de información respecto a sus sistemas de información [1].

2.1.4 Clasificación de la Información

Se buscaron diferentes fuentes que expongan una clasificación de la información en función de lo que SECUINFOR S.A. solicitó, una estructura similar a Pública, Privada, Confidencial. Se observó que los documentos para clasificar la información de esta forma, obedecían más a las

necesidades de cada institución en lugar de a un estándar. Incluso en las políticas de clasificación de las diferentes instituciones encontradas, los niveles de clasificación podían o no obedecer a los tres objetivos de seguridad. En algunas de ellas, la clasificación obedecía únicamente a los criterios de Confidencialidad e Integridad, dejando de lado el criterio de Disponibilidad.

Para este proyecto se escogió el documento de directrices para la clasificación de los datos de la Universidad de Carnegie Mellon. Esta establece el siguiente cuadro para la clasificación de los datos:

Tabla 4: Clasificación de la Datos

Datos Restringidos
Los datos deben ser clasificados como **Restringidos** cuando la revelación no autorizada, alteración y destrucción de los datos, puede causar un riesgo significativo a la institución o sus afiliados. Ejemplos de Datos Restringidos incluyen los datos protegida por el estado, regulaciones federales de privacidad y datos protegidos por acuerdos de confidencialidad. Los controles de seguridad del nivel más alto deben ser aplicados a los datos restringida.
Datos Privados
Los datos deben ser clasificados como **Privados** cuando la revelación no autorizada, alteración y destrucción de los datos, puede resultar en un nivel moderado de riesgo significativo a la institución o sus afiliados. Por defecto, todos los datos institucionales que no está clasificada explícitamente como Restringida o Publica debe ser tratada como Privada. Un nivel razonable de controles de seguridad debe ser aplicado a Los datos Privada.
Datos Publico
Los datos deben ser clasificados como **Públicos** cuando la revelación no autorizada, alteración y destrucción de los datos, puede resultar en un riesgo menor o nulo a la institución o sus afiliados. Ejemplos de Datos Restringidos incluyen las publicaciones de prensa, información de curso, publicaciones de investigaciones. Mientras que poco o ningún control es requerido para proteger la confidencialidad de los datos Públicos, sí se requiere cierto nivel de control para protegerla de la modificación y destrucción no autorizada.

Hasta aquí la información relevante para el proyecto recogida de los estándares y directrices escogidos. Nuestro siguiente paso en el desarrollo de la solución, es la identificación de los activos de información.

2.2 Identificación de la Información

En vista de lo mostrado por los esquemas, estándares y guías investigados, tenemos que primero se necesita la identificación de la información. Específicamente, se aplicará el proceso resultante de este proyecto a la información que tenga valor para la empresa, lo que llamamos "activo de información". Los activos de información de la organización serán entonces aquellos que sirva a la o las funciones principales del negocio. La identificación de la información es tan variable de empresa a empresa, que se considera este proceso como propio de cada organización. Es así que, aunque no es alcance del presente proceso el desarrollo de la identificación de la información, se preguntó las funciones principales de la organización para en función de esto armar un esquema que pueda servir al presente proceso. SECUINFOR S.A. indicó las siguientes como funciones principales:

- Gestionar la seguridad perimetral de los clientes
- Respaldo en Nube de la información propia y de clientes (servicio ofrecido)
- Consultorías de Seguridad Informática: Análisis de Vulnerabilidades y Cómputo Forense

Estas funciones corresponden a los servicios de la empresa. Sin estas operaciones la empresa incumple con los servicios ofrecidos a sus clientes. Se

observa que cada una de las actividades necesita de información la cual trata y gestiona para darle un uso posterior. Esto indica que estas funciones son parte de sistemas de información de SECUINFOR S.A. Entonces hasta el momento se tienen identificadas las funciones principales y por tanto sus sistemas de información. Dentro de estos sistemas de información hay varios tipos de información los cuales contienen a los activos de información que se manejan según el sistema. Se construye la siguiente tabla que asocia los sistemas de información con sus tipos de información a partir de lo indicado por SECUINFOR S.A. y basado en el mapeo que ilustraban la guía de trabajo de mapeo de información de NIST [2]:

Tabla 5: Sistemas de Información y Tipos de Información

SISTEMAS DE INFORMACIÓN	TIPOS DE INFORMACIÓN
Gestión de Seguridad Perimetral	Informes de Gestión y Eventos De estructura y disposición de equipos De Administración de Equipos
Respaldo en Nube	Administración de Equipos Estructura y disposición de equipos Almacenamiento en Equipos Guías y Manuales Técnicos Financiera Administrativa organizacional
Consultorías de Seguridad Informática	Informes de Análisis de Vulnerabilidades Informes de Cómputos Forenses Cotizaciones

SECUINFOR S.A. indica que los servicios se están ampliando, así como las operaciones que realizan. Se desea anotar también que la identificación, tanto de los sistemas como de los tipos de información, no estaba documentada.

2.3 Categorización de Seguridad de la información

Siguiendo lo que las guías adoptadas indican, el siguiente paso, sería la Asignación de niveles de impacto. Puesto que este sub-proceso se realiza para cada objetivo de seguridad, la resultante será la categorización de seguridad de la información. Es así que, para efectos del proceso personalizado para SECUINFOR S.A. se engloba y se nombra al segundo paso: La categorización de seguridad de la información. Para su ejecución se deberán hacer preguntas que permitan seleccionar el nivel de impacto por cada objetivo de seguridad. Se crea entonces un listado de preguntas por cada objetivo de seguridad. Estas preguntas están basadas tanto en el Apéndice A del estándar de clasificación de la información del NYS ITS [4] (Ver también Anexo 5) como en las necesidades de se SECUINFOR S.A. Siguen las tablas de preguntas para la determinación de los impactos por cada objetivo de seguridad:

Tabla 6: Preguntas para determinar Nivel de Impacto de la Confidencialidad

PREGUNTAS DE CONFIDENCIALIDAD	
Para este tipo de información…	
1 La revelación no autorizada impide el funcionamiento de una o más de las funciones primarias de la empresa	
NO	continúe con las preguntas de Confidencialidad
SI	Confidencialidad ALTA, continúe con las preguntas de Integridad
2 La revelación no autorizada causa degradación a una o más de las funciones primarias de la empresa	
No	continúe con las preguntas de Confidencialidad
Si, con impacto limitado	continúe con las preguntas de Confidencialidad
Si, con impacto serio	continúe con las preguntas de Confidencialidad
Si, con impacto severo/catastrófico	Confidencialidad ALTA, continúe con las preguntas de Integridad
3 Qué impacto financiero causa la revelación no autorizada	
Nulo	continúe con las preguntas de Confidencialidad
Impacto limitado	continúe con las preguntas de Confidencialidad
Impacto Serio	continúe con las preguntas de Confidencialidad
Impacto severo/catastrófico	Confidencialidad ALTA, continúe con las preguntas de Integridad
4 ¿Qué impacto causa la revelación no autorizada en la confianza de nuestros clientes?	
Nulo	continúe con las preguntas de Confidencialidad
Impacto limitado	continúe con las preguntas de Confidencialidad
Impacto Serio	continúe con las preguntas de Confidencialidad
Impacto severo/catastrófico	Confidencialidad ALTA, continúe con las preguntas de Integridad
5 ¿La confidencialidad es mandatorio por ley o regulación? De ser así, cual es el impacto de la revelación no autorizada	
No	continúe con las preguntas de Confidencialidad
Si, con impacto limitado	continúe con las preguntas de Confidencialidad
Si, con impacto serio	continúe con las preguntas de Confidencialidad
Si, con impacto severo/catastrófico	Confidencialidad ALTA, continúe con las preguntas de Integridad
6 ¿La distribución debe ser limitada? En caso positivo, cual es el impacto de la revelación no autorizada	
No	continúe con las preguntas de Confidencialidad
Si, con impacto limitado	continúe con las preguntas de Confidencialidad
Si, con impacto serio	continúe con las preguntas de Confidencialidad
Si, con impacto severo/catastrófico	Confidencialidad ALTA, continúe a las preguntas de Integridad
7 ¿Esta información está disponible públicamente?	
NO	Siga las instrucciones de abajo. Luego continúe con las preguntas de Integridad
SI	
Si todas las respuestas son verdes, la clasificación de este tipo de información es **BAJA**	
Si al menos una de las respuestas es amarilla y NINGUNA roja, la clasificación es **MODERADA**	
Si al menos una de las respuestas es roja, la clasificación es **ALTA**	

Tabla 7: Preguntas para determinar Nivel de Impacto de la Integridad

PREGUNTAS DE INTEGRIDAD	
Para este tipo de información…	
1 ¿Se depende de esta información para tomar decisiones críticas de seguridad?	
NO	continúe con las preguntas de Integridad
SI	Integridad ALTA, continúe con las preguntas de Disponibilidad
2 La modificación o destrucción no autorizada impide el funcionamiento de una o más de las funciones primarias de la empresa	
NO	continúe con las preguntas de Integridad
SI	Integridad ALTA, continúe con las preguntas de Disponibilidad
3 La modificación o destrucción no autorizada causa degradación a una o más de las funciones primarias de la empresa	
No	continúe con las preguntas de Integridad
Si, con impacto limitado	continúe con las preguntas de Integridad
Si, con impacto serio	continúe con las preguntas de Integridad
Si, con impacto severo/catastrófico	Integridad ALTA, continúe con las preguntas de Disponibilidad
4 Qué impacto financiero causa la modificación o destrucción no autorizada	
Nulo	continúe con las preguntas de Integridad
Impacto limitado	continúe con las preguntas de Integridad
Impacto Serio	continúe con las preguntas de Integridad
Impacto severo/catastrófico	Integridad ALTA, continúe con las preguntas de Disponibilidad
5 ¿Qué impacto causa la modificación o destrucción no autorizada en la confianza de nuestros clientes?	
Nulo	continúe con las preguntas de Integridad
Impacto limitado	continúe con las preguntas de Integridad
Impacto Serio	continúe con las preguntas de Integridad
Impacto severo/catastrófico	Integridad ALTA, continúe con las preguntas de Disponibilidad
6 ¿La Integridad es mandatorio por ley o regulación? De ser así, cual es el impacto de la modificación o destrucción no autorizada	
No	continúe con las preguntas de Integridad
Si, con impacto limitado	continúe con las preguntas de Integridad
Si, con impacto serio	continúe con las preguntas de Integridad
Si, con impacto severo/catastrófico	Integridad ALTA, continúe con las preguntas de Disponibilidad
7 ¿Se depende de esta información para tomar decisiones del negocio? De ser así, cual es el impacto de la modificación o destrucción no autorizada	
No	
Si, con impacto limitado	Siga las instrucciones de abajo. Luego continúe con las preguntas de Disponibilidad
Si, con impacto serio	
Si, con impacto severo/catastrófico	Integridad ALTA, continúe a las preguntas de Disponibilidad
Si todas las respuestas son verdes, la clasificación de este tipo de información es **BAJA**	
Si al menos una de las respuestas es amarilla y NINGUNA roja, la clasificación es **MODERADA**	
Si al menos una de las respuestas es roja, la clasificación es **ALTA**	

Tabla 8: Preguntas para determinar Nivel de Impacto de la Disponibilidad

PREGUNTAS DE DISPONIBILIDAD	
Para este tipo de información…	
1 La disponibilidad es esencial para la respuesta a emergencia o recuperación de desastre	
NO	continúe con las preguntas de Disponibilidad
SI	Disponibilidad ALTA
2 Debe ser provista o estar disponible	
Como el tiempo lo permita	continúe con las preguntas de Disponibilidad
dentro de 1 a 7 días	continúe con las preguntas de Disponibilidad
24 horas por día / 7 días a la semana	Disponibilidad ALTA
3 La no disponibilidad a tiempo impide el funcionamiento de una o más de las funciones primarias de la empresa	
NO	continúe con las preguntas de Disponibilidad
SI	Disponibilidad ALTA
4 La no disponibilidad a tiempo causa degradación a una o más de las funciones primarias de la empresa	
No	continúe con las preguntas de Disponibilidad
Si, con impacto limitado	continúe con las preguntas de Disponibilidad
Si, con impacto serio	continúe con las preguntas de Disponibilidad
Si, con impacto severo/catastrófico	Disponibilidad ALTA
5 Qué impacto financiero causa la no disponibilidad a tiempo	
Nulo	continúe con las preguntas de Disponibilidad
Impacto limitado	continúe con las preguntas de Disponibilidad
Impacto Serio	continúe con las preguntas de Disponibilidad
Impacto severo/catastrófico	Disponibilidad ALTA
6 ¿Qué impacto causa la no disponibilidad a tiempo en la confianza de nuestros clientes?	
Nulo	continúe con las preguntas de Disponibilidad
Impacto limitado	continúe con las preguntas de Disponibilidad
Impacto Serio	continúe con las preguntas de Disponibilidad
Impacto severo/catastrófico	Disponibilidad ALTA
Si todas las respuestas son verdes, la clasificación de este tipo de información es **BAJA**	
Si al menos una de las respuestas es amarilla y NINGUNA roja, la clasificación es **MODERADA**	
Si al menos una de las respuestas es roja, la clasificación es **ALTA**	

Por cada tabla se obtendrá un valor de impacto del tipo de información según el objetivo de seguridad. Así, se puede completar la categoría de seguridad del tipo de información:

$$SC_{\text{tipo de información}} = \{(\text{confidencialidad, impacto resultante de la aplicación de la Tabla 6}), (\text{integridad, impacto resultante de la aplicación de la Tabla 7}), (\text{disponibilidad, impacto resultante de la aplicación de la Tabla 8})\} \quad (2.5)$$

2.4 Clasificación de la información

Este sería el paso final del proceso para que su salida sea en el formato solicitado por la organización. Como se anotó previamente, no había estándares para la clasificación de la data, sino más bien que esta clasificación va ajustada a las necesidades de cada organización. Entonces, para SECUINFOR S.A. se establece como criterios de clasificación de los activos de información los tres objetivos de seguridad.

Se seguirán tres niveles de clasificación: Pública, Privada y Restringida. Con fines de uso en SECUINFOR S.A., se ajusta la definición de estas en función de los impactos y de las categorías ya establecidas. Por tanto:

Tabla 9: Criterios de Clasificación de la Información

Información Restringida
Deberá ser clasificada como Restringida aquella información para la cual el no cumplimiento de uno o más objetivos de seguridad, represente impacto severo o catastrófico para la organización. Una información deberá ser clasificada Restringida si AL MENOS UNO de los niveles de impacto de la categorización del tipo de información al que pertenece es ALTO.
Información Privada
Deberá ser clasificada como Privada aquella información para la cual el no cumplimiento de uno o más objetivos de seguridad, represente impacto serio para la organización. Una información deberá ser clasificada Privada si AL MENOS UNO de los niveles de impacto de la categorización del tipo de información al que pertenece es MODERADO y NINGUNO de los niveles es ALTO
Información Publica
Podrá ser clasificada como Pública aquella información para la cual el no cumplimiento de uno o más objetivos de seguridad, represente impacto menor o nulo para la organización. Una información podrá ser clasificada como Publica si TODOS los niveles de impacto de la categorización del tipo de información al que pertenece son BAJOS

La siguiente tabla es una guía de ayuda para la determinación de la clasificación de la información, a partir de la categoría de seguridad:

Tabla 10: Determinación de la Clasificación del Tipo de Información

Si en la categoría de seguridad…	La información es
Los niveles de impacto de confidencialidad, integridad y disponibilidad son BAJOS	PUBLICA
Al menos uno de los niveles de impacto para la confidencialidad, integridad o disponibilidad es MODERADO y NINGUNO es ALTO	PRIVADA
Al menos uno de los niveles de impacto de la confidencialidad, integridad y disponibilidad es ALTO	RESTRINGIDA

2.5 Proceso final de clasificación de la información: Pasos generales.

El desarrollo del proceso nos llevó a aterrizar el mismo en los siguientes pasos generales:

1. ENTRADA: Sistema de Información identificado
2. Identificar el tipo de Información
3. Categorizar el tipo información
4. Clasificar el tipo de información
5. SALIDA: Activo de información clasificado

Cada uno de estos pasos tienen entradas y generan salidas y por ello pueden considerarse también sub-procesos. Se describen brevemente entonces las fases del proceso en definición:

2.5.1 Identificación del sistema de información

Entrada del proceso general. Comprende la elección del sistema de información al cual pertenece el activo de información a clasificar. Los sistemas de información se encuentran detallados en la Tabla 5.

2.5.2 Identificación del tipo de información

En esta etapa del proceso, se determina el tipo de información al que pertenece el activo que es objeto de este proceso. En la misma tabla 5 se

encuentran los tipos de información asociados a los sistemas de información.

2.5.3 Categorización de Seguridad del tipo de información

En esta fase dentro del proceso, se establece la categoría de seguridad del tipo de información. Es decir, el nivel de impacto asociado para cada objetivo de seguridad. Se obtiene realizando las preguntas de las tablas 6, 7 y 8 para el tipo de información. El resultado tendrá el formato de SC:

$$SC_{\text{tipo de información}} = \{(\text{confidencialidad, impacto}), (\text{integridad, impacto}), (\text{disponibilidad, impacto})\} \quad (2.6)$$

2.5.4 Clasificación del Activo de Información

Este sub-proceso busca establecer finalmente la clasificación del activo de información como Pública, Privada o Restringida, mediante los lineamientos de la tabla 9 y aplicando la tabla 10 a la categoría de seguridad. Es necesario recordar que todos los activos de información específicos tendrán la misma clasificación que el tipo de información donde se encuentran contenidos. Es decir, al clasificar el tipo de Información, clasifico también el activo que lo contiene. El resultado de este sub-proceso será el activo de información clasificado. Se recomienda el uso de un documento de registro de clasificación de la información. Se provee un formato ejemplo en el Anexo 1 de este proyecto.

CAPÍTULO 3

RESULTADOS

En este capítulo se esquematiza el proceso desarrollado en el Capítulo 2. Se lo detalla en gráfico para su fácil aplicación. Finalmente, se realiza una prueba del proceso para clasificar dos activos de información escogidos por SECUINFOR S.A.

3.1 Proceso de Clasificación de Activos de Información para SECUINFOR S.A.

Los siguientes son los esquemas que muestran el proceso final aterrizado. Estos son entregables a SECUINFOR S.A. para su aplicación y registro en la documentación. Primero tenemos el proceso general en visión macro:

Figura 3.1: Proceso de Clasificación de los Activos de Información

Y el siguiente recuadro presenta el proceso en detalle con las actividades que se deben ejecutar:

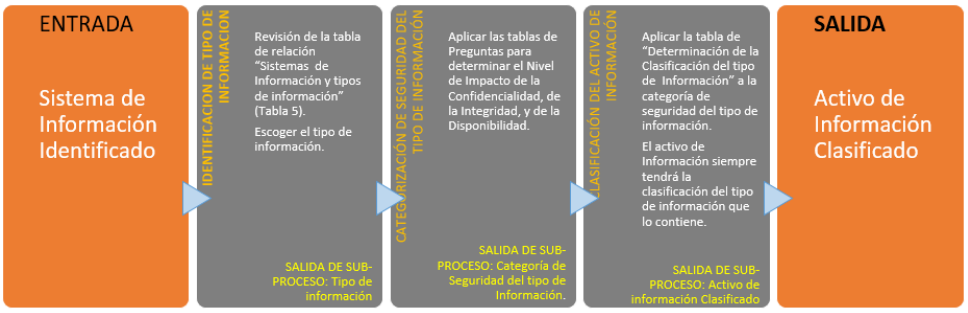


Figura 3.2: Proceso de Clasificación de los Activos de Información

3.2 Prueba del Proceso

Se aplicó el presente proceso a dos activos de información para prueba de resultados.

El primer activo escogido es un **archivo de claves** que corresponde al sistema de Respaldo en Nube. La **ENTRADA** del proceso entonces es el sistema de información identificado: Respaldo en Nube.

A continuación, en conjunto con Personal de SECUINFOR S.A. se realizó la **IDENTIFICACIÓN DEL TIPO DE INFORMACIÓN** que es el activo archivo de claves. Recurrimos a la tabla de sistemas y tipos de información para la identificación:

SISTEMAS DE INFORMACION	TIPOS DE INFORMACION
Gestion de Seguridad Perimetral	Informes de Gestión y Eventos De estructura y disposición de equipos De Administración de Equipos
Respaldo en Nube	Administración de Equipos Estructura y disposición de equipos Almacenamiento en Equipos Guías y Manuales Técnicos Financiera Administrativa organizacional
Consultorias de Seguridad Informatica	Informes de Análisis de Vulnerabilidades Informes de Cómputos Forenses Cotizaciones

Figura 3.3: Identificación del tipo de Información del activo "archivo de claves"

Como resultado de este sub-proceso se obtuvo la identificación del tipo de información.

El siguiente paso del proceso es la **CATEGORIZACIÓN DE SEGURIDAD DEL TIPO DE INFORMACIÓN**. En conjunto con el personal de SECUINFOR se aplicaron las preguntas de confidencialidad, integridad y disponibilidad, para determinar los niveles de impacto de este tipo de información:

PREGUNTAS DE CONFIDENCIALIDAD	
Para este tipo de información...	
1 La revelación no autorizada impide el funcionamiento de una o más de las funciones primarias	
✓ NO	continúe con las preguntas de Confidencialidad
SI	Confidencialidad ALTA, continúe con las preguntas de Integridad
2 La revelación no autorizada causa degradación a una o más de las funciones primarias de la	
✓ No	continúe con las preguntas de Confidencialidad
Si, con impacto limitado	continúe con las preguntas de Confidencialidad
Si, con impacto serio	continúe con las preguntas de Confidencialidad
Si, con impacto severo/catastrófico	Confidencialidad ALTA, continúe con las preguntas de Integridad
3 Qué impacto financiero causa la revelación no autorizada	
✓ Nulo	continúe con las preguntas de Confidencialidad
Impacto limitado	continúe con las preguntas de Confidencialidad
Impacto Serio	continúe con las preguntas de Confidencialidad
Impacto severo/catastrófico	Confidencialidad ALTA, continúe con las preguntas de Integridad
4 ¿Qué impacto causa la revelación no autorizada en la confianza de nuestros clientes?	
Nulo	continúe con las preguntas de Confidencialidad
Impacto limitado	continúe con las preguntas de Confidencialidad
Impacto Serio	continúe con las preguntas de Confidencialidad
✓ Impacto severo/catastrófico	**Confidencialidad ALTA, continúe con las preguntas de Integridad**

Figura 3.4: Preguntas de Confidencialidad del Tipo de Información "Administración de Equipos"

En la cuarta pregunta, se determinó el impacto ALTO del objetivo de seguridad Confidencialidad. Entonces tenemos que:

$$SC_{\text{Administración de Equipos}} = \{(\text{confidencialidad}, \text{ALTA}), (\text{integridad}, ¿?), (\text{disponibilidad}, ¿?)\} \quad (3.1)$$

Como fue indicado por la tabla anterior continuamos con las preguntas de Integridad:

PREGUNTAS DE INTEGRIDAD	
Para este tipo de información…	
1 Se depende de esta información para tomar decisiones críticas de seguridad?	
✓ NO	continúe con las preguntas de Integridad
SI	Integridad ALTA, continúe con las preguntas de Disponibilidad
2 La modificación o destrucción no autorizada impide el funcionamiento de una o más de las funciones primarias de la empresa	
NO	continúe con las preguntas de Integridad
✓ SI	**Integridad ALTA, continúe con las preguntas de Disponibilidad**

Figura 3.5: Preguntas de Integridad del Tipo de Información "Administración de Equipos"

En la segunda pregunta se determinó el impacto ALTO del objetivo de seguridad Integridad para este tipo de Información. Hasta este punto, tenemos que:

$$SC_{\text{Administración de Equipos}} = \{(\text{confidencialidad, ALTA}), (\text{integridad, ALTA}), (\text{disponibilidad, ¿?})\} \quad (3.2)$$

Continuamos con las preguntas de Disponibilidad:

PREGUNTAS DE DISPONIBILIDAD	
Para este tipo de información…	
1 La disponibilidad es esencial para la respuesta a emergencia o recuperación de desastre	
NO	continúe con las preguntas de Disponibilidad
✓ SI	**Disponibilidad ALTA**

Figura 3.6: Preguntas de Disponibilidad del Tipo de Información "Administración de Equipos"

En la primera pregunta se determinó el impacto ALTO del objetivo de seguridad Disponibilidad para este tipo de Información. Es así que tenemos completa la Categoría de Seguridad para el tipo de Información Administración de Equipos:

$$SC_{\text{Administración de Equipos}} = \{(\text{confidencialidad, ALTA}), (\text{integridad, ALTA}), (\text{disponibilidad, ALTA})\} \quad (3.3)$$

El siguiente paso en nuestro proceso es la **CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN**. Para el efecto usamos la tabla de Determinación de la Clasificación del Tipo de Información aplicándola a la SC del tipo de Información que se está trabajando "Administración de Equipos".

Si...	La información es
Los niveles de impacto de confidencialidad, integridad y disponibilidad son BAJOS	PUBLICA
Al menos uno de los niveles de impacto para la confidencialidad, integridad o disponibilidad es MODERADO y NINGUNO es ALTO	PRIVADA
Al menos uno de los niveles de impacto de la confidencialidad, integridad y disponibilidad es ALTO	**RESTRINGIDA**

Figura 3.7 Clasificación del tipo de Información "Administración de Equipos"

Se obtuvo entonces que el tipo de información "Administración de Equipos" del sistema de información "Respaldo en Nube" tiene clasificación Restringida.

Puesto que un activo de información es parte de un tipo de información, este activo tendrá la categorización de seguridad y la clasificación que tenga su tipo de información. Es así que, nuestro activo de información **archivo de claves** tendrá también clasificación **Restringida**.

El segundo activo escogido es un **guía de Administración** que corresponde al sistema de Gestión de Seguridad Perimetral. La **ENTRADA** del proceso entonces es el sistema de información identificado: Respaldo en Nube.

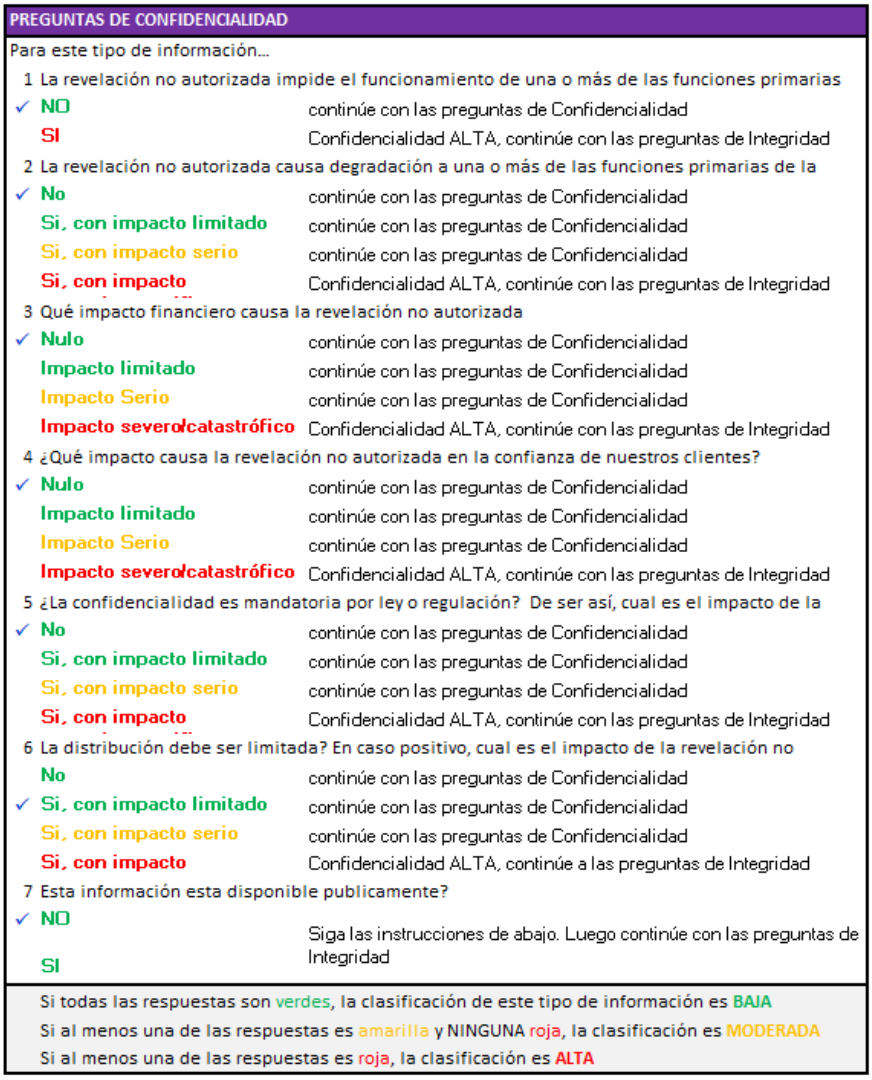
A continuación, en conjunto con Personal de SECUINFOR S.A. se realizó la **IDENTIFICACIÓN DEL TIPO DE INFORMACIÓN** que es el activo Guía de Administración. Recurrimos a la tabla de sistemas y tipos de información para la identificación:

SISTEMAS DE INFORMACION	TIPOS DE INFORMACION
Gestion de Seguridad Perimetral	Informes de Gestión y Eventos De estructura y disposición de equipos De Administración de Equipos
Respaldo en Nube	Administración de Equipos Estructura y disposición de equipos Almacenamiento en Equipos Guías y Manuales Técnicos Financiera Administrativa organizacional
Consultorias de Seguridad Informatica	Informes de Análisis de Vulnerabilidades Informes de Cómputos Forenses Cotizaciones

Figura 3.8: Identificación del tipo de Información del activo "Guía de Administración"

Como resultado de este sub-proceso se obtuvo la identificación del tipo de información. Este activo pertenece al tipo de información: Guías y Manuales Técnicos

El siguiente paso del proceso es la **CATEGORIZACIÓN DE SEGURIDAD DEL TIPO DE INFORMACIÓN**. En conjunto con el personal de SECUINFOR S.A. se aplicaron las preguntas de confidencialidad, integridad y disponibilidad, para determinar los niveles de impacto de este tipo de información:



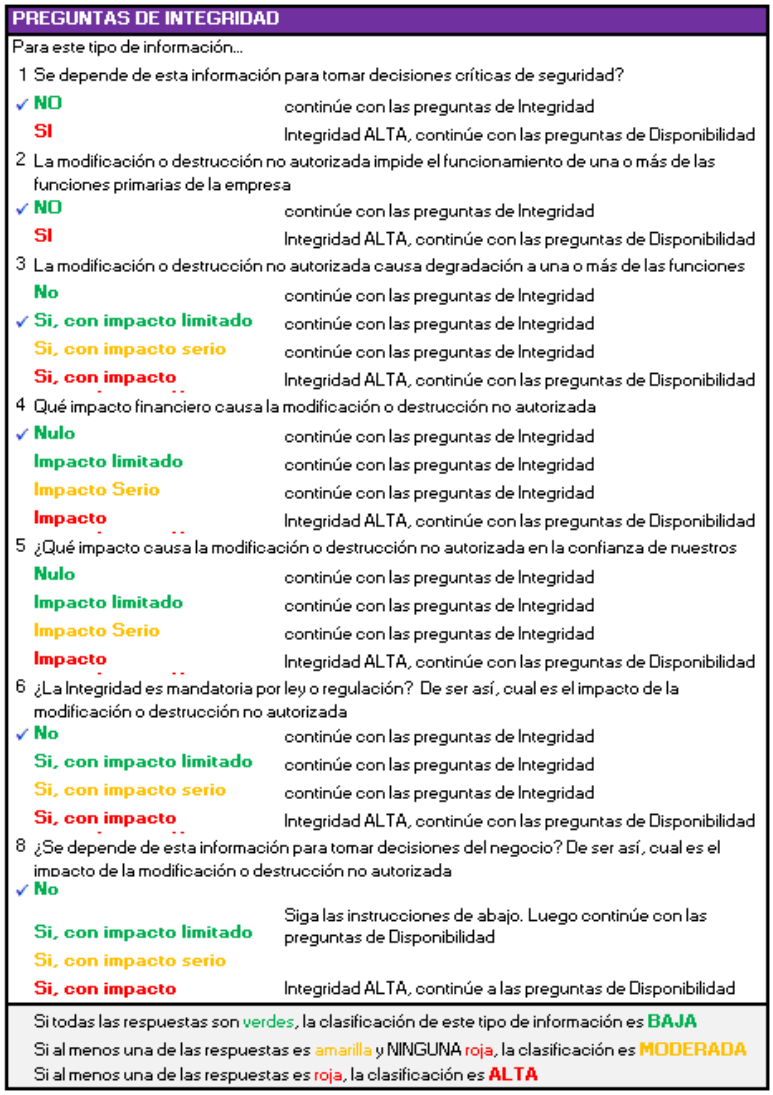
PREGUNTAS DE CONFIDENCIALIDAD	
Para este tipo de información...	
1 La revelación no autorizada impide el funcionamiento de una o más de las funciones primarias	
✓ NO	continúe con las preguntas de Confidencialidad
SI	Confidencialidad ALTA, continúe con las preguntas de Integridad
2 La revelación no autorizada causa degradación a una o más de las funciones primarias de la	
✓ No	continúe con las preguntas de Confidencialidad
Si, con impacto limitado	continúe con las preguntas de Confidencialidad
Si, con impacto serio	continúe con las preguntas de Confidencialidad
Si, con impacto	Confidencialidad ALTA, continúe con las preguntas de Integridad
3 Qué impacto financiero causa la revelación no autorizada	
✓ Nulo	continúe con las preguntas de Confidencialidad
Impacto limitado	continúe con las preguntas de Confidencialidad
Impacto Serio	continúe con las preguntas de Confidencialidad
Impacto severo/catastrófico	Confidencialidad ALTA, continúe con las preguntas de Integridad
4 ¿Qué impacto causa la revelación no autorizada en la confianza de nuestros clientes?	
✓ Nulo	continúe con las preguntas de Confidencialidad
Impacto limitado	continúe con las preguntas de Confidencialidad
Impacto Serio	continúe con las preguntas de Confidencialidad
Impacto severo/catastrófico	Confidencialidad ALTA, continúe con las preguntas de Integridad
5 ¿La confidencialidad es mandatoria por ley o regulación? De ser así, cual es el impacto de la	
✓ No	continúe con las preguntas de Confidencialidad
Si, con impacto limitado	continúe con las preguntas de Confidencialidad
Si, con impacto serio	continúe con las preguntas de Confidencialidad
Si, con impacto	Confidencialidad ALTA, continúe con las preguntas de Integridad
6 La distribución debe ser limitada? En caso positivo, cual es el impacto de la revelación no	
No	continúe con las preguntas de Confidencialidad
✓ Si, con impacto limitado	continúe con las preguntas de Confidencialidad
Si, con impacto serio	continúe con las preguntas de Confidencialidad
Si, con impacto	Confidencialidad ALTA, continúe a las preguntas de Integridad
7 Esta información esta disponible publicamente?	
✓ NO	Siga las instrucciones de abajo. Luego continúe con las preguntas de Integridad
SI	
Si todas las respuestas son verdes, la clasificación de este tipo de información es BAJA	
Si al menos una de las respuestas es amarilla y NINGUNA roja, la clasificación es MODERADA	
Si al menos una de las respuestas es roja, la clasificación es ALTA	

Figura 3.9: Preguntas de Confidencialidad del Tipo de Información "Guías y Manuales Técnicos"

Al finalizar todas las preguntas, se determinó el impacto BAJO del objetivo de seguridad Confidencialidad. Entonces tenemos que:

SC Guías y Manuales Técnicos = {(confidencialidad, BAJA), (integridad, ¿?), (disponibilidad, ¿?)} (3.4)

Continuamos con las preguntas de Integridad:



PREGUNTAS DE INTEGRIDAD

Para este tipo de información...

1 Se depende de esta información para tomar decisiones críticas de seguridad?

✓ NO	continúe con las preguntas de Integridad
SI	Integridad ALTA, continúe con las preguntas de Disponibilidad

2 La modificación o destrucción no autorizada impide el funcionamiento de una o más de las funciones primarias de la empresa

✓ NO	continúe con las preguntas de Integridad
SI	Integridad ALTA, continúe con las preguntas de Disponibilidad

3 La modificación o destrucción no autorizada causa degradación a una o más de las funciones

No	continúe con las preguntas de Integridad
✓ Si, con impacto limitado	continúe con las preguntas de Integridad
Si, con impacto serio	continúe con las preguntas de Integridad
Si, con impacto	Integridad ALTA, continúe con las preguntas de Disponibilidad

4 Qué impacto financiero causa la modificación o destrucción no autorizada

✓ Nulo	continúe con las preguntas de Integridad
Impacto limitado	continúe con las preguntas de Integridad
Impacto Serio	continúe con las preguntas de Integridad
Impacto	Integridad ALTA, continúe con las preguntas de Disponibilidad

5 ¿Qué impacto causa la modificación o destrucción no autorizada en la confianza de nuestros

Nulo	continúe con las preguntas de Integridad
Impacto limitado	continúe con las preguntas de Integridad
Impacto Serio	continúe con las preguntas de Integridad
Impacto	Integridad ALTA, continúe con las preguntas de Disponibilidad

6 ¿La Integridad es mandatoria por ley o regulación? De ser así, cual es el impacto de la modificación o destrucción no autorizada

✓ No	continúe con las preguntas de Integridad
Si, con impacto limitado	continúe con las preguntas de Integridad
Si, con impacto serio	continúe con las preguntas de Integridad
Si, con impacto	Integridad ALTA, continúe con las preguntas de Disponibilidad

8 ¿Se depende de esta información para tomar decisiones del negocio? De ser así, cual es el impacto de la modificación o destrucción no autorizada

✓ No	
Si, con impacto limitado	Siga las instrucciones de abajo. Luego continúe con las preguntas de Disponibilidad
Si, con impacto serio	
Si, con impacto	Integridad ALTA, continúe a las preguntas de Disponibilidad

Si todas las respuestas son verdes, la clasificación de este tipo de información es **BAJA**
Si al menos una de las respuestas es amarilla y NINGUNA roja, la clasificación es **MODERADA**
Si al menos una de las respuestas es roja, la clasificación es **ALTA**

Figura 3.10: Preguntas de Integridad del Tipo de Información "Guías y Manuales Técnicos"

Al finalizar las preguntas, se determinó el impacto BAJO del objetivo de seguridad Integridad para este tipo de Información. Hasta esta instancia, tenemos que:

$$SC_{\text{Guías y Manuales Técnicos}} = \{(\text{confidencialidad, BAJA}), (\text{integridad, BAJA}), (\text{disponibilidad, ¿?})\} \quad (3.5)$$

Continuamos con las preguntas de Disponibilidad:

PREGUNTAS DE DISPONIBILIDAD	
Para este tipo de información...	
1 La disponibilidad es esencial para la respuesta a emergencia o recuperación de desastre	
✓ NO	continúe con las preguntas de Disponibilidad
SI	Disponibilidad ALTA
2 Debe ser provista o estar disponible	
Como el tiempo lo permita	continúe con las preguntas de Disponibilidad
✓ dentro de 1 a 7 dias	continúe con las preguntas de Disponibilidad
24 hrs por día / 7 dias a la semana	Disponibilidad ALTA
3 La no disponibilidad a tiempo impide el funcionamiento de una o más de las funciones primarias de la empresa	
✓ NO	continúe con las preguntas de Disponibilidad
SI	Disponibilidad ALTA
4 La no disponibilidad a tiempo causa degradación a una o más de las funciones primarias de la empresa	
✓ No	continúe con las preguntas de Disponibilidad
Si, con impacto limitado	continúe con las preguntas de Disponibilidad
Si, con impacto serio	continúe con las preguntas de Disponibilidad
Si, con impacto severo/catastrófico	Disponibilidad ALTA
5 Qué impacto financiero causa la no disponibilidad a tiempo	
Nulo	continúe con las preguntas de Disponibilidad
✓ Impacto limitado	continúe con las preguntas de Disponibilidad
Impacto Serio	continúe con las preguntas de Disponibilidad
Impacto severo/catastrófico	Disponibilidad ALTA
6 ¿Qué impacto causa la no disponibilidad a tiempo en la confianza de nuestros clientes?	
Nulo	continúe con las preguntas de Disponibilidad
✓ Impacto limitado	continúe con las preguntas de Disponibilidad
Impacto Serio	continúe con las preguntas de Disponibilidad
Impacto severo/catastrófico	Disponibilidad ALTA
Si todas las respuestas son verdes, la clasificación de este tipo de información es BAJA	
Si al menos una de las respuestas es amarilla y NINGUNA roja, la clasificación es MODERADA	
Si al menos una de las respuestas es roja, la clasificación es ALTA	

Figura 3.11: Preguntas de Disponibilidad del Tipo de Información "Guías y Manuales Técnicos"

Al finalizar las preguntas, se determinó el impacto MODERADO del objetivo de seguridad Disponibilidad para este tipo de Información. Es así que tenemos completa la Categoría de Seguridad para el tipo de Información "Guías y Manuales Técnicos":

$$SC_{\text{Guía y Manuales Técnicos}} = \{(\text{confidencialidad, BAJA}), (\text{integridad, BAJA}), (\text{disponibilidad, MODERADA})\} \quad (3.6)$$

El siguiente paso en nuestro proceso es la **CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN**. Para el efecto usamos la tabla de Determinación de la Clasificación del Tipo de Información aplicándola a la SC del tipo de Información que se está trabajando "Guías y Manuales Técnicos".

Si...	La información es
Los niveles de impacto de confidencialidad, integridad y disponibilidad son BAJOS	PUBLICA
Al menos uno de los niveles de impacto para la confidencialidad, integridad o disponibilidad es MODERADO y NINGUNO es ALTO	PRIVADA
Al menos uno de los niveles de impacto de la confidencialidad, integridad y disponibilidad es ALTO	**RESTRINGIDA**

Figura 3.12: Clasificación del tipo de Información "Guías y Manuales Técnicos"

Se obtuvo entonces que el tipo de información “Guías y Manuales Técnicos” del sistema de información “Respaldo en Nube” tiene clasificación Privada. Puesto que un activo de información es parte de un tipo de información, este activo tendrá la categorización de seguridad y la clasificación que tenga su tipo de información. Es así que, nuestro activo de información **Guía de Administración** tendrá también clasificación **Privada**.

3.3 Análisis de Resultados

De las dos pruebas realizadas, tenemos que el proceso propició la determinación de la clasificación de dos activos de información diferentes.

- El activo de información “archivo de claves” del sistema de Información de Respaldo en Nube resultó clasificado como Restringido
- El activo de información “Guía Administrativa” del mismo sistema de información resultó clasificado como Privado.

A pesar de pertenecer al mismo sistema de información, los resultados fueron distintos como se esperaba ya que ambos tipos de información no tienen el mismo impacto para la empresa.

SECUINFOR S.A. se mostró conforme con los resultados del proceso y confirmaron la aplicabilidad del mismo. La empresa cuenta ahora con un apoyo para poder definir el tratamiento que se le debe dar a sus activos de información en función de su clasificación. Esto a su vez, facilitará a la empresa la toma de

decisiones estratégicas en cuanto a las medidas de protección que vayan a tomar.

Se pudo observar que conforme las operaciones de SECUINFOR S.A. vayan incrementándose, también deberá crecer el cuadro de Mapeo de Sistemas de Información y Tipos de Información.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. El proceso definido mediante el presente proyecto cumple su objetivo: la clasificación de los activos de información del centro de operaciones de seguridad SECUINFOR S.A. como Publica, Privada y Restringida

2. El proceso resultado de este proyecto está apoyado en estándares internacionales; usa como criterios de categorización y clasificación los tres pilares de la Seguridad Informática: la Confidencialidad, Integridad, y Disponibilidad y está adaptado a las necesidades y requerimientos de la empresa.

3. La salida de este proceso (el activo de información clasificado) permitirá a SECUINFOR S.A. determinar los tratamientos y controles adecuados para sus activos de información, y a su vez facilitará la toma de decisiones estratégicas en

cuanto a las medidas de protección de su información. Esto era parte del problema planteado al principio del proyecto.

4. SECUINFOR S.A. cuenta ahora con un proceso de clasificación de su información, esto es un paso para arrancar el proceso de preparación para la certificación ISO 27001 que la empresa persigue en el mediano plazo. El presente proceso encaja en el objetivo de control A.7.2.1 Directrices de Control de esta Norma. Esto era parte del problema planteado al principio del proyecto

5. El proceso de clasificación de los activos de información es escalable y adaptable. La clasificación sugerida en el presente proceso (Pública, Privada, Restringida) puede ser ampliada según vayan cambiando las necesidades de la empresa, sin mayor modificación a las fases principales del proceso. Así mismo, según vayan creciendo los requerimientos de la empresa las preguntas de Confidencialidad, Integridad y Disponibilidad pueden ser más exhaustivas y específicas.

Recomendaciones

1. Este proceso necesita sólidas entradas referentes a la información identificada. Se observó que la identificación de la información de la empresa no está documentada. No existían tampoco registros físicos donde se encuentren enumerados los sistemas de información de la empresa. Esta información se encontraba al inicio de este proyecto solo como parte del conocimiento del personal de SECUINFOR S.A. Durante el desarrollo del presente proceso, se descubrió la necesidad de tener registrados, documentados o al menos listados

los sistemas de información de la organización. Se creó un mapeo para que pueda servir al proceso en creación, pero este mapeo puede estar limitado si no se han considerado todos los activos de información que posee la organización. Se recomienda fuertemente la creación de un proceso de identificación de los sistemas de información y de sus tipos de información para que puedan servir de manera óptima a otros procesos relacionados a la información de la empresa.

2. Los niveles de impacto financiero a la empresa no estaban definidos de manera específica. SECUINFOR S.A. facilitaba niveles de impacto subjetivos y acorde a la experiencia y conocimiento de los directivos, mas no existía un estudio documentado del impacto financiero. Se recomienda fuertemente la realización de un estudio del impacto financiero que tendría la perdida de la confidencialidad, integridad o disponibilidad de la información.

3. Se recomienda la creación de un súper proceso de tratamiento de la información que contenga al presente proceso de Clasificación de los activos de información. De esta forma, se puede obtener retroalimentación del actual proceso e identificar puntos de mejora.

4. Se recomienda la revisión regular de este proceso, o bajo demanda según vayan incrementando las necesidades de la empresa.

BIBLIOGRAFÍA

[1] National Institute of Standards and Technology, US Department of Commerce. (2004). Standards for Security Categorization of Federal Information and Information System. FIPS PUB 199. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf fecha de consulta febrero del 2016

[2] National Institute of Standards and Technology, US Department of Commerce. (2008) Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories. SP 800-60. http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf fecha de consulta febrero del 2016

[3] National Institute of Standards and Technology, US Department of Commerce. (2008) Volume II: Guide for Mapping Types of Information and Information Systems to Security Categories. SP 800-60. http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf fecha de consulta febrero del 2016

[4] New York State Office of Information Technology Services. (2014). Information Technology Standard Information Classification. NYS-S14-002. https://its.ny.gov/sites/default/files/documents/Enterprise_Information_Classification_v3_1.pdf fecha de consulta febrero del 2016

[5] Carnegie Mellon University, Information Security Office. (2015). Guidelines for Data Classification. http://www.cmu.edu/iso/governance/guidelines/data-classification.html, fecha de consulta febrero 2016

[6] Poveda, José Manuel. Módulo 7: Los activos de Seguridad de la Información. http://www.worldvisioncapacitacion.cl/wp-

content/uploads/cursos_adjuntos/f52e0bd4c6c2c203413952826f916237.pdf, fecha de consulta febrero 2016

ANEXOS

Anexo 1. Formato Propuesto para Registro de Clasificación de Activos de Información

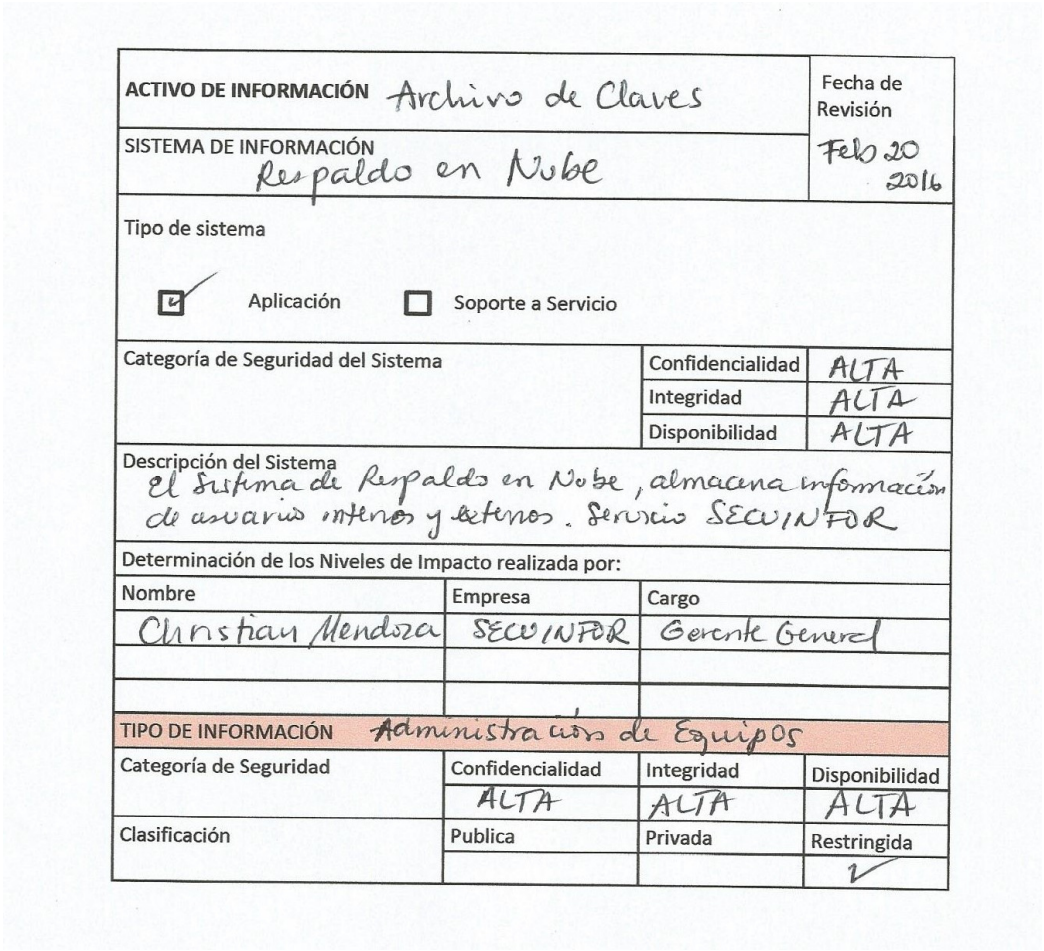
<table>
<tr><td colspan="3">ACTIVO DE INFORMACIÓN</td><td>Fecha de Revisión</td></tr>
<tr><td colspan="3">SISTEMA DE INFORMACIÓN</td><td></td></tr>
<tr><td colspan="4">Tipo de sistema

☐ Aplicación ☐ Soporte a Servicio</td></tr>
<tr><td colspan="2" rowspan="3">Categoría de Seguridad del Sistema</td><td>Confidencialidad</td><td></td></tr>
<tr><td>Integridad</td><td></td></tr>
<tr><td>Disponibilidad</td><td></td></tr>
<tr><td colspan="4">Descripción del Sistema</td></tr>
<tr><td colspan="4">Determinación de los Niveles de Impacto realizada por:</td></tr>
<tr><td>Nombre</td><td>Empresa</td><td colspan="2">Cargo</td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="4">TIPO DE INFORMACIÓN</td></tr>
<tr><td rowspan="2">Categoría de Seguridad</td><td>Confidencialidad</td><td>Integridad</td><td>Disponibilidad</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td rowspan="2">Clasificación</td><td>Publica</td><td>Privada</td><td>Restringida</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

Anexo 2. Formato Propuesto para Registro de Clasificación de Sistemas de Información y Tipos de Información

SISTEMA DE INFORMACIÓN		Fecha de revisión	
Tipo de sistema ☐ Aplicación ☐ Soporte a Servicio			
Categoría de Seguridad del Sistema		Confidencialidad	
		Integridad	
		Disponibilidad	
Descripción del Sistema			
Determinación de los Niveles de Impacto realizada por:			
Nombre	Empresa	Cargo	
TIPO DE INFORMACIÓN			
Categoría de Seguridad	Confidencialidad	Integridad	Disponibilidad
Clasificación	Publica	Privada	Restringida
TIPO DE INFORMACIÓN			
Categoría de Seguridad	Confidencialidad	Integridad	Disponibilidad
Clasificación	Publica	Privada	Restringida
TIPO DE INFORMACIÓN			
Categoría de Seguridad	Confidencialidad	Integridad	Disponibilidad
Clasificación	Publica	Privada	Restringida

Anexo 3. Formato Registro de Clasificación de Activo de Información: Archivo de Claves



ACTIVO DE INFORMACIÓN Archivo de Claves			Fecha de Revisión
SISTEMA DE INFORMACIÓN Respaldo en Nube			Feb 20 2016
Tipo de sistema ☑ Aplicación ☐ Soporte a Servicio			
Categoría de Seguridad del Sistema		Confidencialidad	ALTA
		Integridad	ALTA
		Disponibilidad	ALTA
Descripción del Sistema: El Sistema de Respaldo en Nube, almacena información de usuarios internos y externos. Servicio SECUINFOR			
Determinación de los Niveles de Impacto realizada por:			
Nombre	Empresa	Cargo	
Christian Mendoza	SECUINFOR	Gerente General	
TIPO DE INFORMACIÓN Administración de Equipos			
Categoría de Seguridad	Confidencialidad	Integridad	Disponibilidad
	ALTA	ALTA	ALTA
Clasificación	Publica	Privada	Restringida
			✓

Anexo 4. Formato Registro de Clasificación de Activo de Información: Archivo de Claves

ACTIVO DE INFORMACIÓN Guía de Administración			Fecha de Revisión
SISTEMA DE INFORMACIÓN Respaldo en Nube			Feb 20 2016
Tipo de sistema ☑ Aplicación ☐ Soporte a Servicio			
Categoría de Seguridad del Sistema		Confidencialidad	ALTA
		Integridad	ALTA
		Disponibilidad	ALTA
Descripción del Sistema			
Determinación de los Niveles de Impacto realizada por:			
Nombre	Empresa	Cargo	
Christian Mendoza	SECUINFOR	Gerente General	
TIPO DE INFORMACIÓN Guías y Manuales Técnicos			
Categoría de Seguridad	Confidencialidad	Integridad	Disponibilidad
	BAJA	BAJA	MODERADA
Clasificación	Publica	Privada	Restringida
		✓	

Anexo 5. Hoja de Trabajo para la Clasificación de Activos del Standard de Clasificación de Activos del NYS ITS.

INFORMATION ASSET CLASSIFICATION WORKSHEET — **Appendix A**

CIA QUESTIONS

CONFIDENTIALITY QUESTIONS	INTEGRITY QUESTIONS	AVAILABILITY QUESTIONS
1 Does the information include or contain PPSI (Personal, Private, or Sensitive Information)? **A) No** - continue with Confidentiality questions **D) Yes** - Confidentiality is High (rate below), continue with Integrity questions	**1 Does the information include medical records?** **A) No** - continue with Integrity questions **D) Yes** - Integrity is High (rate below), continue with Availability questions	**1 Is availability of the information essential for emergency response or disaster recovery?** **A) No** - continue with Availability questions **D) Yes** - Availability is High (rate below)
2 What impact does unauthorized access or disclosure of information have on health and safety? **A) None** - continue with Confidentiality questions **B) Limited impact** - continue with Confidentiality questions **C) Serious impact** - continue with Confidentiality questions **D) Severe Impact** - Confidentiality is High (rate below), continue with Integrity questions	**2 Is the information (e.g., security logs) relied upon to make critical security decisions ?** **A) No** - continue with Integrity questions **D) Yes** - Integrity is High (rate below), continue with Availability questions	**2 This information needs to be provided or available:** **A) As time permits** - continue with Availability questions **C) Within 1 to 7 days** - continue with Availability questions **D) 24 hrs. per day/7 days a week** - Availability is High (rate below)
3 What is the financial impact of unauthorized access or disclosure of information? **A) None** - continue with Confidentiality questions **B) Limited impact** - continue with Confidentiality questions **C) Serious impact** - continue with Confidentiality questions **D) Severe Impact** - Confidentiality is High (rate below), continue with Integrity questions	**3 What impact does unauthorized modification or destruction of information have on health and safety?** **A) None** - continue with Integrity questions **B) Limited impact** - continue with Integrity questions **C) Serious impact** - continue with Integrity questions **D) Severe Impact** - Integrity is High (rate below), continue with Availability questions	**3 What is the impact to health and safety if information were not available when needed?** **A) None** - continue with Availability questions **B) Limited impact** - continue with Availability questions **C) Serious impact** - continue with Availability questions **D) Severe Impact** - Availability is High (rate below)
4 What impact does unauthorized access or disclosure of information have on the SE mission? **A) None** - continue with Confidentiality questions **B) Limited impact** - continue with Confidentiality questions **C) Serious impact** - continue with Confidentiality questions **D) Severe Impact** - Confidentiality is High (rate below), continue with Integrity questions	**4 What is the financial impact of unauthorized modification or destruction of information?** **A) None** - continue with Integrity questions **B) Limited impact** - continue with Integrity questions **C) Serious impact** - continue with Integrity questions **D) Severe Impact** - Integrity is High (rate below), continue with Availability questions	**4 What is the financial impact if information were not available when needed?** **A) None** - continue with Availability questions **B) Limited impact** - continue with Availability questions **C) Serious impact** - continue with Availability questions **D) Severe Impact** - Availability is High (rate below)
5 What impact does unauthorized access or disclosure of information have on the public trust? **A) None** - continue with Confidentiality questions **B) Limited impact** - continue with Confidentiality questions **C) Serious impact** - continue with Confidentiality questions **D) Severe Impact** - Confidentiality is High (rate below), continue with Integrity questions	**5 What impact does unauthorized modification or destruction of information have on the SE mission?** **A) None** - continue with Integrity questions **B) Limited impact** - continue with Integrity questions **C) Serious impact** - continue with Integrity questions **D) Severe Impact** - Integrity is High (rate below), continue with Availability questions	**5 What is the impact to the SE mission if information were not available when needed?** **A) None** - continue with Availability questions **B) Limited impact** - continue with Availability questions **C) Serious impact** - continue with Availability questions **D) Severe Impact** - Availability is High (rate below)
6 Is confidentiality mandated by law or regulation? If yes, determine the impact of unauthorized access or disclosure of information. **A) No** - continue with Confidentiality questions **B) Yes - Limited impact** - continue with Confidentiality questions **C) Yes - Serious impact** - continue with Confidentiality questions **D) Yes - Severe impact** - Confidentiality is High (rate below), continue with Integrity questions	**6 What impact does unauthorized modification or destruction of information have on the public trust?** **A) None** - continue with Integrity questions **B) Limited impact** - continue with Integrity questions **C) Serious impact** - continue with Integrity questions **D) Severe impact** - Integrity is High (rate below), continue with Availability questions	**6 What is the impact to the public trust if the information were not available when needed?** **A) None** - see Instructions below **B) Limited impact** - see Instructions below **C) Serious impact** - see Instructions below **D) Severe impact** - Availability is High (rate below)
7 Is the information intended for limited distribution? If yes, determine the impact of unauthorized access or disclosure. **A) No** - continue with Confidentiality questions **B) Yes - Limited impact** - continue with Confidentiality questions **C) Yes - Serious impact** - continue with Confidentiality questions **D) Yes - Severe impact** - Confidentiality is High (rate below), continue with Integrity questions	**7 Is integrity addressed by law or regulation? If yes, determine the impact of unauthorized modification or destruction of information.** **A) No** - continue with Integrity questions **B) Yes - Limited impact** - continue with Integrity questions **C) Yes - Serious impact** - continue with Integrity questions **D) Yes - Severe impact** - Integrity is High (rate below), continue with Availability ques.	
8 Is the information publicly available? **A) No** - see Instructions below, then continue with Integrity questions **B) Yes** - see Instructions below, then continue with Integrity questions	**8 Is the information (e.g., financial transactions, performance appraisals) relied upon to make business decisions? If yes, determine the impact of unauthorized modification or destruction of information.** **A) No** - see Instructions below then continue with Availability questions **B) Yes - Limited impact** - see Instructions below then continue with Availability ques. **C) Yes - Serious impact** - see Instructions below then continue with Availability ques. **D) Yes - Severe impact** - Integrity is High (rate below), continue with Availability ques.	
INSTRUCTIONS FOR RATING EACH COLUMN: If ALL of the above answers are A/B (GREEN), rating is LOW; If ANY of the above answers are C (YELLOW) and NONE are D (RED), rating is MODERATE; If ANY of the above answers are D (RED), rating is HIGH SCALE: A/B = GREEN = LOW C = YELLOW = MODERATE D = RED = HIGH		
CLASSIFICATION RATING FOR CONFIDENTIALITY:	CLASSIFICATION RATING FOR INTEGRITY:	CLASSIFICATION RATING FOR AVAILABILITY: