

SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN – TALLER

1

SISTEMAS DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN

ING. JOHN ROBERTH CORREA

INTEGRANTES DEL GRUPO:

LUIS FELIPE VELASCO TAO

JUAN DAVID GONZALEZ DIMATÉ

UNIVERSIDAD DE SAN BUENAVENTURA


FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS

BOGOTÁ

11 DE MARZO

2021


	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 1 SGSI	2021 - 1
---	--	---------------	----------

Versión del documento

Fecha	Consideraciones
9 de marzo 2021	Versión inicial del documento. Incluye descripción de la organización, marco legal, alcances, misión, core del negocio, clientes y proveedores. Activos planteados, pero no definidos. Información sobre seguridad y activos no definida (Matrices).
10 de marzo 2021	Activos definidos, Información sobre seguridad y activos definida (matrices).
14 de marzo 2021	Evaluación de riesgos realizada, Matriz de calificación, evaluación y respuesta a los riesgos realizada, Tabla de valoración de controles realizada. Mapa de riesgos realizado.

Contenido

Sistema de gestión de la seguridad de la información	3
Descripción del negocio.....	3
Tipo de empresa	3
Razón social.....	3
Acta de constitución	5
Política de constitución.....	7
Alcance	7
Misión.....	7
Core del negocio	8
Clientes y proveedores.....	8
Activos de información.....	8
Activos de infraestructura tecnológica.....	8
Activos de información críticos y misionales.	9
Identificación de responsables sobre los activos	10
Activos de infraestructura tecnológica.....	10
Activos de información críticos y misionales	11

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 1 SGSI	2021 - 1
---	--	---------------	----------

Evaluación de riesgos	12
Criterio de probabilidad.....	13
Criterio de Impacto.	13
Estado actual de la seguridad de la entidad	15
Matriz de riesgos y vulnerabilidades de infraestructura tecnológica.	15
Matriz de calificación, evaluación y respuesta a los riesgos.	15
Valoración de controles	15
Matriz de riesgos de los activos.....	17

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

En este documento se realizará la actividad de la materia de Sistemas de gestión de la seguridad en la cual se implementará un SGSI para una empresa.

Descripción del negocio

En este apartado se describirá la naturaleza del negocio en el cual se implementará el sistema de información de modo tal conozcamos como profesionales las particularidades de la empresa.


Tipo de empresa

Nuestra empresa se encuentra dirigida por Luis Felipe Velasco y Juan David González constituida como una sociedad anónima, clasificada como una empresa pequeña ya que solo contamos con un grupo de profesionales de 25 empleados, nuestra actividad se clasifica en el sector terciario debido a que prestamos el servicio de desarrollo de software, y teniendo hasta el momento un nivel de alcance local en la ciudad de Bogotá.


Razón social

Soft-easy S.A es una empresa colombiana ubicada en la ciudad de Bogotá la cual cuenta con un equipo de ingenieros, técnicos y tecnólogos capacitados en la creación de software para pequeña y media empresa de todo el país, prestando servicios como el



 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 1 SGSI	2021 - 1
--	--	----------------------	-----------------

desarrollo de sistemas contables, aplicaciones móviles, web e híbridas, siempre pensando en nuestros clientes, sus necesidades y el deseo de un país cada vez más digital.

	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 1 SGSI	2021 - 1
---	--	---------------	----------

Acta de constitución

ACTA DE CONSTITUCION DE SOFT-EASY S.A

En la ciudad de Soft-Easy, siendo las 9:10 a.m. del día 9 del mes 3, del año 2021, se reúnen las siguientes personas con el propósito de constituir SOFT-EASY S.A:

NOMBRES	TIPO DE DOCUMENTO	NUMERO DE IDENTIFICACION	DOMICILIO (municipio de residencia)
Luis Felipe Velasco Tao	Cedula de ciudadanía	1010200300	Calle siempreviva 12 - 10
Juan David González	Cedula de ciudadanía	1121547896	Calle olmo 20 - 121

Orden del Día:

1. Designación de presidente y secretario/a de la reunión.
2. Manifestación de voluntad de constituir una empresa en sociedad anónima.
3. Aprobación de los Estatutos.
4. Nombramiento de Representante Legal, Junta Directiva y Revisor Fiscal.
5. Lectura y aprobación del texto integral del acta.

1. DESIGNACION DE PRESIDENTE Y SECRETARIO DE LA REUNION.


Se nombran para estos cargos a:

Presidente: Carmen Torres, identificado con CC No. 36852147

Secretario: Juan Pérez, identificado con CC No. 45789123

2. MANIFESTACIÓN DE VOLUNTAD DE CONSTITUIR UNA SOCIEDAD ANONIMA.

Los constituyentes relacionados en la presente acta manifiestan su voluntad de constituir una empresa en sociedad anónima, del tipo privada, persona jurídica de derecho privado, de las reguladas, en lo pertinente, por el Decreto 2150 de 1995, el

	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 1 SGSI	2021 - 1
---	--	---------------	----------

Decreto 427 de 1996 y demás disposiciones especiales, denominada xxxxxxxxx y cuya sigla será xx

3. APROBACION DE LOS ESTATUTOS

El presidente de la reunión hace énfasis que, para la constitución de la entidad sin ánimo de lucro, se han observado todas las disposiciones legales vigentes y se han conformado los estatutos según lo indicado en las normas especiales que la regulan.

Una vez elaborados y analizados los estatutos de la empresa en sociedad anónima que se constituye, los constituyentes y/o fundadores dieron su APROBACIÓN por unanimidad. Los estatutos se adjuntan a la presente acta y forman parte integral de la misma.

4. NOMBRAMIENTO DE DIRECTIVOS, REPRESENTANTE LEGAL Y ORGANOS DE FISCALIZACIÓN (FISCAL, REVISOR FISCAL).

De conformidad con lo previsto en los estatutos que rigen a la entidad, se APROBÓ por unanimidad la designación de las siguientes personas para integrar sus órganos de administración y fiscalización:

a. Representante Legal:

Nombre completo: Luis Felipe Velasco Tao

Tipo de documento de identificación Cedula de ciudadanía


No. del documento de identificación 1010200300

Fecha de expedición del documento de identificación (D/M/A) 20/11/2019

b. Junta Directiva:

Principales:

NOMBRE COMPLETO	TIPO DE DOCUMENTO DE IDENTIFICACION	NO. DEL DOCUMENTO DE IDENTIFICACIÓN	FECHA DE EXPEDICION DEL DOCUMENTO DE IDENTIFICACION (DD/MM/AA)	CARGO
Pepita Pérez	CC	58741693	15/04/2010	Jefe de producción

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 1 SGSI	2021 - 1
--	--	----------------------	-----------------

Pepito Pérez	CC	74123587	08/08/2008	Jefe de asesorías
--------------	----	----------	------------	----------------------

c. Revisor Fiscal

Nombre completo: Rafael Castro

Tipo de documento de identificación CC

No. del documento de identificación 95753159

Fecha de expedición del documento de identificación (D/M/A) 19/06/1998

No. de la tarjeta profesional 1478523

La(s) persona(s) nombrada(s) estando presente(s) acepta(n) el cargo para el cual ha(n) sido designada(s).

6. LECTURA Y APROBACIÓN DEL ACTA

Sometida a consideración de los constituyentes, la presente acta fue leída y aprobada y en constancia de todo lo anterior se firma por el presidente y secretario de la reunión.

PRESIDENTE

C.C. 36852147

SECRETARIO

C.C. 45789123

Política de constitución


Pendiente

Alcance

“Para el 2030 se proyecta a Soft-easy como una empresa con presencia a nivel nacional, con un cuerpo de trabajo presente en las principales ciudades de Colombia”

Misión

“Brindarle a la mediana y pequeña empresa la oportunidad de acceder a software que le facilite la administración y gestión de sus procesos”

 <p>UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ</p>	<p>Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información</p>	<p>TALLER 1 SGSI</p>	<p>2021 - 1</p>
---	--	----------------------	-----------------

Core del negocio

Desarrollo de software (aplicaciones web, móvil, híbridas, programas de escritorio)

Clientes y proveedores

En este apartado se definen posibles clientes que podría tener nuestra empresa, pensando también en nuestro público objetivo y las necesidades que puede tener este, además de pensar de empresas externas las cuales nos provean servicios para nuestro correcto funcionamiento.

Posibles clientes

Como posibles clientes siempre se abarcará a la pequeña y mediana empresa sin importar su actividad económica, listando algunos ejemplos se mencionan a:

- Tiendas de ropa
- Oficinas de abogados
- Tiendas de alimentos
- Cafeterías y restaurantes
- Pequeños prestadores de servicios (domicilios, aseo, mantenimiento, etc.)

Estos clientes pueden requerir aplicaciones web o móviles y/o páginas web para la interacción con sus clientes, gestión de sus ingresos, clientes, productos y demás actividades propias ya de cada empresa.

Proveedores

Como principales proveedores requeridos para Soft-easy tenemos definidos a los siguientes:


- Prestador de servicio de electricidad
- Prestador de servicio de internet
- Mantenimiento de zonas comunes
- Github: plataforma de hosting para código fuente.

Activos de información

A continuación, se mencionarán los activos de información que hacen funcionar a Soft-easy. Estos activos son una parte fundamental de la empresa, ya que constituyen los recursos físicos y lógicos que la empresa tiene a su disposición para su funcionamiento.

Activos de infraestructura tecnológica

Son los activos que están conformados por los equipos físicos que tiene a disposición Soft-easy. Esto incluye: Ordenadores, Cableado y Servidores. A continuación, se explicarán estos activos con más detalle.

 <p>UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ</p>	<p>Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información</p>	<p>TALLER 1 SGSI</p>	<p>2021 - 1</p>
---	--	----------------------	-----------------

Equipos de la oficina principal

Son los ordenadores que todo empleado tiene a su disposición en la empresa. En la oficina principal ubicada en la ciudad de Bogotá D.C se encontrarán diez equipos, de los cuales dos están destinados para la recepción de proyectos, y ocho están destinados para el desarrollo de los proyectos recibidos previamente. Puede consultar el anexo B para más información.

Red local de la oficina principal

Es la red que conecta cada ordenador y servidor dentro de la empresa. Provee el servicio de comunicación entre dispositivos dentro de la empresa, necesario para realizar un gran número de tareas. Puede consultar el anexo B para más información.

Servidor web

Es el servidor que gestiona el servicio que ofrece la empresa en la red. Servidor destinado para el almacenamiento de los servicios web de la empresa, en este caso la aplicación web y sus componentes CSS, JS, PHP y HTML. Puede consultar el anexo B para más información.

Servidor de archivos

Es el servidor que almacena los archivos y/o documentos que la empresa maneja. Servidor destinado para el almacenamiento de archivos y documentación requerida para el desarrollo de los proyectos de cada uno de los clientes. Puede consultar el anexo B para más información.

Servidor de base de datos


Es el servidor destinado para el almacenamiento de las bases de datos requeridas para el negocio (Base de datos de clientes y estado de los proyectos). Puede consultar el anexo B para más información.

Activos de información críticos y misionales.

Son los activos relacionados a la propia información que maneja la empresa. Este activo contiene la información relacionada con la propia empresa, sus empleados, sus clientes, sus proyectos y los datos vinculados a estos aspectos. De cierta manera esos activos son el objetivo principal de protección del SGSI, que intenta mantenerlos lo más íntegros y confidenciales posible.

Bases de datos

Son el conjunto de estructuras por medio de las cuales se almacenarán los datos requeridos para el correcto funcionamiento de la empresa. Puede consultar el anexo B para más información.

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 1 SGSI	2021 - 1
---	--	---------------	----------

Aplicación web del negocio

Es el software por medio del cual se le prestara a los clientes servicios como vigilar los avances o el estado de sus proyectos, petición de citas y muestra de proyectos previos que les sirvan a los clientes para conocer la calidad de los productos de nuestra empresa. Puede consultar el anexo B para más información.

Repositorio Git para proyectos

Es el Software en la nube por medio del cual se almacenará el código fuente de los proyectos, que sirvan de apoyo para futuros clientes y nuevos trabajadores en la empresa. Puede revisar el anexo B para más información.

Datos de empleados y clientes

Son todo el conjunto de información almacenada en las bases de datos y servidor de archivos requerida para la gestión de los clientes y de nuestros empleados. Puede consultar el anexo B para más información.

Identificación de responsables sobre los activos


Para el correcto uso y mantenimiento de los activos utilizados por Soft-easy, los siguientes miembros del personal estarán encargados de gestionarlos.

Los responsables detallados en el siguiente apartado deberán entenderse como:

- Desarrollador: Persona empleada en Soft-easy que presta sus conocimientos en desarrollo de software a la empresa.
- Personal de mantenimiento: Persona empleada en Soft-easy que presta sus conocimientos sobre redes y computadoras a la empresa.
- Analista de datos: Persona empleada en Soft-easy que presta sus conocimientos sobre bases de datos y gestión de la información a la empresa.
- Especialista de seguridad: Persona empleada en Soft-easy que presta sus conocimientos sobre seguridad informática a la empresa.

Activos de infraestructura tecnológica

1. Equipos de la oficina principal: Los desarrolladores empleados por Soft-easy deben encargarse de darle buen uso a los equipos de la empresa, el personal de mantenimiento deberá encargarse de realizar la configuración correspondiente a los equipos, que incluye todas las dependencias y sub-dependencias que lo componen y el especialista de seguridad deberá encargarse de configurar los equipos de manera segura. Esto incluye la instalación de un antivirus y la configuración del firewall. Las dependencias mencionadas anteriormente se detallan en el anexo B.
2. Red local de la oficina principal: El personal de mantenimiento deberá encargarse de configurar adecuadamente la red local de la empresa,


 <p>UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ</p>	<p>Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información</p>	<p>TALLER 1 SGSI</p>	<p>2021 - 1</p>
---	--	----------------------	-----------------

asegurándose que no existan errores de conexión y/o fallas estructurales que impidan la correcta comunicación entre todos los equipos físicos de la empresa.

3. Servidor web: El personal de mantenimiento deberá encargarse de configurar y establecer el servidor web, de manera que se conecte con la red local. Además, deberá asegurarse que su ubicación sea segura y que no esté afectado en gran medida por condiciones ambientales, meteorológicas y/o estructurales, tales como: Goteras, espacios aislados, plagas de insectos, entre otros.
4. Servidor de archivos: Revisar servidor web.
5. Servidor de bases de datos: El analista de datos deberá encargarse de realizar una correcta instalación del servidor, junto con una supervisión rigurosa del mismo. El personal de mantenimiento deberá encargarse de establecer una correcta conexión entre el servidor y los equipos de la organización.

Activos de información críticos y misionales

1. Bases de datos: El analista de información debe encargarse de configurar adecuadamente el motor de BD correspondiente en cada equipo que esté utilizando la empresa, además de realizar un chequeo regular para verificar que la información que se esté utilizando por el personal general de la empresa sea auténtica.
2. Aplicación web del negocio: Los desarrolladores de la empresa deben encargarse de configurar adecuadamente la aplicación web, y someterla a mejoras y actualizaciones continuamente para su correcto funcionamiento. Además de esto, deben seguir los estándares para la escritura de código seguro propuestos por el especialista de seguridad.
3. Repositorio Git para proyectos: Los desarrolladores deben guardar cualquier información relacionada con los proyectos en curso en el repositorio Git de la empresa. El repositorio Git será configurado por el especialista de seguridad con el fin de que la información almacenada aquí sea lo más confidencial posible.
4. Datos de empleados y clientes: El especialista en seguridad deberá capacitar a todo el personal sobre los posibles ataques que pueden sufrir con el fin de robar información sobre ellos o la empresa, tales como el Phishing. Además, deberá diseñar un plan de acción para el personal en tal caso que estos ataques ocurran.

 <p>UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ</p>	<p>Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información</p>	<p>TALLER 1 SGSI</p>	<p>2021 - 1</p>
---	--	----------------------	-----------------


EVALUACIÓN DE RIESGOS

En este apartado se realizará un primer control sobre el estado de la seguridad de la empresa Soft-easy, estableciendo unos lineamientos concretos para la evaluación de los riesgos que puedan llevarse a cabo en ella. Estos lineamientos son:

- **Criterio de probabilidad:** Se entiende como la probabilidad de ocurrencia del riesgo, la cual puede ser medida con criterios de frecuencia o factibilidad. En el criterio de frecuencia se analizan el número de ventos en un periodo determinado, mientras que en el criterio de factibilidad se analiza la presencia de factores internos y externos que pueden propiciar el riesgo.
- **Nivel de impacto:** Se tienen en cuenta las consecuencias potenciales que pueden ocasionar un nivel de afectación sobre los activos de la entidad.

También hay que tener en cuenta que existen varias clases de riesgos que pueden afectar a la seguridad de la empresa, y el tener la información de esto permite realizar un control más eficiente. Las clases de riesgo son:

- **Riesgo estratégico:** Se asocia con la forma en que se administra la Entidad, su manejo se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
- **Riesgos de Imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
- **Riesgos Operativos:** Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.
- **Riesgos financieros:** Se relacionan con el manejo de los recursos de la entidad que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
- **Riesgos de Cumplimientos:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
- **Riesgos de Tecnología:** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
- **Riesgos de Corrupción:** Relacionados con acciones, omisiones, uso indebido del poder, de los recursos o de la información para la obtención de un beneficio particular o de un tercero.


	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 1 SGSI	2021 - 1
---	--	---------------	----------

Criterio de probabilidad.


Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	El evento ocurrirá en la mayoría de las circunstancias.	Más de una vez al año
4	Probable	El evento puede ocurrir en la mayoría de las circunstancias.	Al menos una vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos una vez en los últimos dos años.
2	Rara vez	El evento puede ocurrir en algún momento.	Al menos una vez en los últimos tres años.
1	Imposible	El evento puede ocurrir sólo en circunstancias especiales	No se ha presentado en los últimos cinco años

Criterio de Impacto.

Nivel	Descriptor	Impacto Cuantitativo	Impacto cualitativo
5	Catastrófico	<ul style="list-style-type: none"> - Impacto que afecte la ejecución presupuestal en un valor $\geq 50\%$ - Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 50\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 50\%$ - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 50\%$ del presupuesto general de la entidad. 	<ul style="list-style-type: none"> - Interrupción de las operaciones de la Entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de Información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
4	Mayor	<ul style="list-style-type: none"> - Impacto que afecte la ejecución presupuestal en un valor $\geq 20\%$ - Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 20\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 20\%$ 	<ul style="list-style-type: none"> - Interrupción de las operaciones de la Entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.

 <p>UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ</p>	<p>Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información</p>	<p>TALLER 1 SGSI</p>	<p>2021 - 1</p>
---	--	----------------------	-----------------

		<ul style="list-style-type: none"> - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 20\%$ del presupuesto general de la entidad 	<ul style="list-style-type: none"> - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos
3	Moderado	<ul style="list-style-type: none"> - Impacto que afecte la ejecución presupuestal en un valor $\geq 5\%$ - Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 10\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 5\%$ - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 5\%$ del presupuesto general de la entidad. 	<ul style="list-style-type: none"> - Interrupción de las operaciones de la Entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
2	Menor	<ul style="list-style-type: none"> - Impacto que afecte la ejecución presupuestal en un valor $\leq 1\%$ - Pérdida de cobertura en la prestación de los servicios de la entidad $\leq 5\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\leq 1\%$ - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\leq 1\%$ del presupuesto general de la entidad. 	<ul style="list-style-type: none"> - Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
1	Insignificante	<ul style="list-style-type: none"> - Impacto que afecte la ejecución presupuestal en un valor $\leq 0,5\%$ - Pérdida de cobertura en la prestación de los servicios de la entidad $\leq 1\%$. 	<ul style="list-style-type: none"> - No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 1 SGSI	2021 - 1
--	--	----------------------	-----------------

	<ul style="list-style-type: none"> - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\leq 0,5\%$ - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\leq 0,5\%$ del presupuesto general de la entidad. 	
--	---	--

Estado actual de la seguridad de la entidad

El estado de seguridad actual de la entidad se detalla en el **anexo A**. Las métricas definidas en el documento son las que se van a evaluar con detenimiento para identificar los riesgos que estén afectando a la empresa.

Matriz de riesgos y vulnerabilidades de infraestructura tecnológica.

En el **anexo B** se identifican los riesgos que afectan a los activos de información que posee la empresa. Con base en esto, se realizará el análisis correspondiente para conocer el impacto que estos riesgos y vulnerabilidades tienen en la organización.

Matriz de calificación, evaluación y respuesta a los riesgos.


Para esta matriz se tendrán que establecer criterios de evaluación para clasificar cada riesgo que pueda existir. Los criterios pueden establecerse con un Mapa de riesgos consolidado, como el de la siguiente figura.

Probabilidad	Impacto				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E
B= Zona de riesgo baja: Se asume el riesgo. M= Zona de riesgo moderada: Asumir el riesgo Reducir el riesgo. A= Zona de riesgo alto: Reducir el riesgo, Evitar, Compartir o Transferir E= Zona de riesgo Extremo: Reducir el riesgo, Evitar, Compartir o Transferir					

En el **anexo C** se encuentra definida la matriz de calificación, evaluación y respuesta de todos los riesgos identificados en los **anexos A y B**.

Valoración de controles

Para un adecuado tratamiento de riesgos, es necesario evaluar los controles a aplicar en ellos. Para este apartado se requieren establecer criterios para definir si

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 1 SGSI	2021 - 1
--	--	----------------------	-----------------

el control a utilizar en un riesgo es el más adecuado para tratarlo. Estos criterios pueden definirse mediante una tabla de valoración de controles con la siguiente estructura:


Descripción del control	Criterios para la evaluación	Evaluación		Observaciones
		Sí	No	
Describa el control determinado para el riesgo identificado	¿El control previene la materialización del riesgo (afecta probabilidad)? ¿El control permite enfrentar la situación en caso de materialización (afecta impacto)?	N/A	N/A	Este criterio no puntúa, es relevante determinar si el control es preventivo (probabilidad) o si es correctivo que permite enfrentar el evento una vez materializado (impacto), con el fin de establecer el desplazamiento en la matriz de evaluación de riesgos.
	¿Existen manuales, instructivos o procedimientos para el manejo del control?	15	0	
	¿Está(n) definido(s) el(los) responsable(s) de la ejecución del control y del seguimiento?	5	0	
	¿El control es automático? (Sistemas o Software que permiten incluir contraseñas de acceso, o con controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros).	15	0	
Describa el control determinado para el riesgo identificado	¿El control es manual? (Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros)	10	0	
	¿La frecuencia de ejecución del control y seguimiento es adecuada?	15	0	
	¿Se cuenta con evidencias de la ejecución y seguimiento del control?	10	0	
	¿En el tiempo que lleva la herramienta ha demostrado ser efectiva?	30	0	
	TOTAL	100	0	

Para verificar si el control a implementar puede o no ser utilizado para tratar un determinado riesgo se puede utilizar la siguiente tabla:

Tabla para evaluación de riesgos según valoración de controles.

RANGOS DE CLASIFICACIÓN DE LOS CONTROLES	DEPENDIENDO SI EL CONTROL AFECTA PROBABILIDAD O IMPACTO SE DESPLAZA EN LA MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS.	
	CUADRANTE A DISMINUIR EN LA PROBABILIDAD	CUADRANTE A DISMINUIR EN EL IMPACTO
ENTRE 0-50	0	0
ENTRE 51-75	1	1
ENTRE 76-100	2	2

En el **anexo D** se encuentran detalladas las valoraciones a los controles de riesgo que se identificaron. Véase que solamente se consideraron los controles que: 1) Están definidos en el **anexo A** de la NTC ISO-IEC 27001 y 2) Eran los más

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 1 SGSI	2021 - 1
--	--	----------------------	-----------------

adecuados para realizar acciones correctivas y preventivas a los riesgos identificados

Matriz de riesgos de los activos

Para finalizar, la matriz de riesgos de los activos detallada en el **anexo E** permite visualizar los riesgos identificados como riesgos inherentes (es decir, su forma al ser identificados por primera vez) y riesgos residuales (su forma después de haberles implementado los controles respectivos), de modo que permita comprender la relación entre los controles a implementar y los riesgos a disminuir.