uts Unidades Tecnológicas de Santander

¡Lo hacemos posible!

POLÍTICA INSTITUCIONAL DE
ADMINISTRACIÓN DEL RIESGO
UNIDADES TECNOLÓGICAS DE SANTANDER

Adriana Vanegas Aguilar
Jefe Oficina de Planeación
Representante de la Dirección

uts Unidades Tecnológicas de Santander
¡Lo hacemos posible!

POLÍTICA INSTITUCIONAL DE
ADMINISTRACIÓN DEL RIESGO

UNIDADES TECNOLÓGICAS DE SANTANDER

Documento Versión 2

POLÍTICA INSTITUCIONAL

ADMINISTRACIÓN DEL RIESGO

UNIDADES TECNOLÓGICAS DE SANTANDER

ESTRUCTURA GENERAL

Lineamientos de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V.5

Modelo Integrado de Planeación y Gestión en los Procesos **MIPG**

Política

Institucional de Administración del Riesgo UTS

Estructura del Sistema Integrado de Gestión - **SIG**

Modelo Estándar de Control Interno **MECI**

POLÍTICA INSTITUCIONAL
ADMINISTRACIÓN DEL RIESGO
UNIDADES TECNOLÓGICAS DE SANTANDER

POLÍTICA
La Política Institucional de Administración del Riesgo se define como la expresión del compromiso del equipo directivo frente a la identificación, valoración, y tratamiento de los riesgos y oportunidades, acciones que se obtienen como resultado de la gestión realizada por la institución, con el propósito de alcanzar de manera eficaz y efectiva el logro de los objetivos y la misión institucional

OBJETIVO
Contribuir a la seguridad razonable frente al cumplimiento de la misión y al logro de los objetivos institucionales, mediante la asignación de roles y responsabilidades de cada uno de los servidores públicos y contratistas de prestación de servicios de la Institución y adopción de lineamientos para el tratamiento, manejo y seguimiento a los riesgos de *gestión, corrupción, y seguridad digital,* para la administración de riesgos de las UTS.

Administración del riesgo

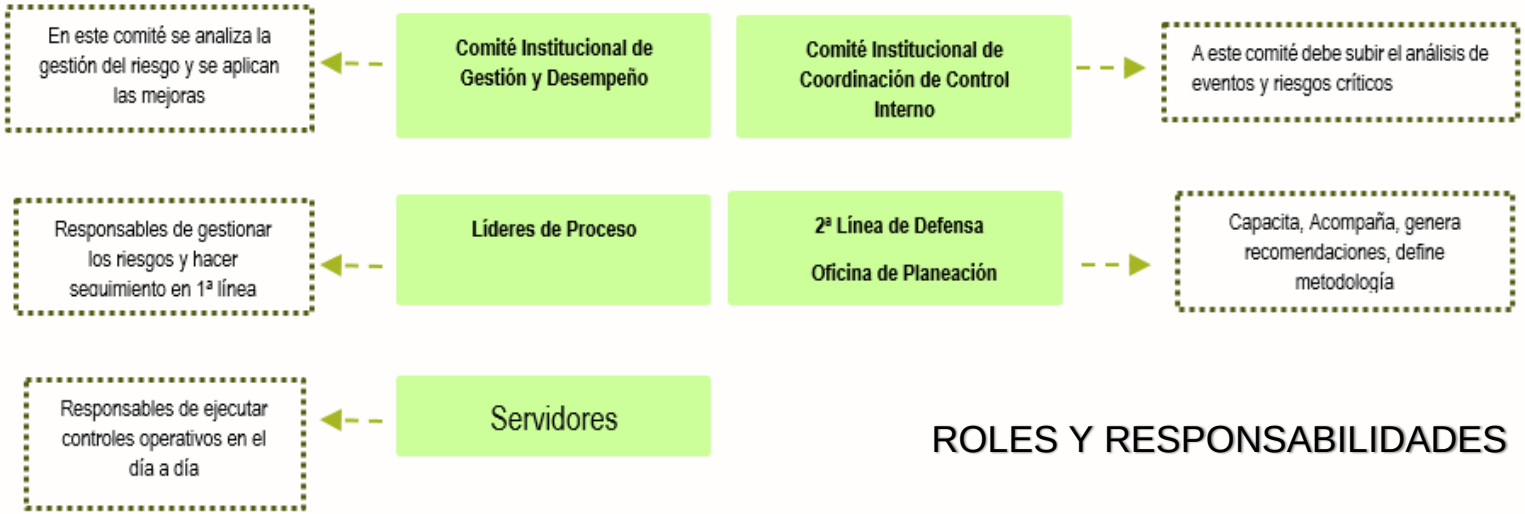
Lineamientos

- Establecer la metodología que permita administrar los riesgos de gestión, de corrupción y de seguridad de la información
- Asegurar los recursos necesarios para ayudar a los responsables a gestionar el riesgo

POLÍTICA INSTITUCIONAL
ADMINISTRACIÓN DEL RIESGO
UNIDADES TECNOLÓGICAS DE SANTANDER

ÁMBITO DE APLICACIÓN

Esta política aplica a todos los procesos, a los planes institucionales, a los programas, a los proyectos y a las acciones ejecutadas por los servidores públicos y contratistas de prestación de servicios de las Unidades Tecnológicas de Santander, durante el ejercicio de sus funciones y obligaciones, respectivamente.



ROLES Y RESPONSABILIDADES

POLÍTICA INSTITUCIONAL

ADMINISTRACIÓN DEL RIESGO

UNIDADES TECNOLÓGICAS DE SANTANDER

LINEAMIENTOS PARA RIESGOS DE GESTIÓN

1.1. Identificación del riesgo

1.2. Valoración del riesgo

1.3. Valoración de controles

1.4. Evaluación de riesgos

1.5. Estrategias para combatir el riesgo

1.6. Riesgos asociados a la continuidad de negocio

1.7. Monitoreo y Seguimiento

1.1. Identificación del riesgo

1. Análisis de Objetivos Estratégicos y de los procesos.

2. Identificación de los puntos de riesgo

3. Identificación de áreas de impacto.

4. Identificación de áreas de factores de Riesgo

- ☑ Procesos
- ☑ Talento Humano
- ☑ Tecnología
- ☑ Infraestructura
- ☑ Eventos externos (Terceros)

5. Descripción del Riesgo

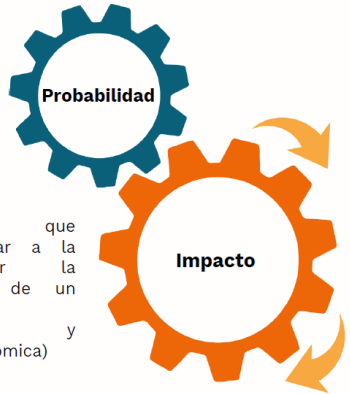
6. Clasificación del Riesgo

POLÍTICA INSTITUCIONAL
ADMINISTRACIÓN DEL RIESGO
UNIDADES TECNOLÓGICAS DE SANTANDER

LINEAMIENTOS PARA RIESGOS DE GESTIÓN

1.2. Valoración del Riesgo

La probabilidad se basa en el número de veces en que se pasa por el punto de riesgo en el período de un año.



Consecuencias que puede ocasionar a la entidad por la materialización de un riesgo.
(Reputacional y afectación económica)

Definición Controles (Medida que permite reducir o mitigar un riesgo)

Probabilidad

	Frecuencia de la Actividad	Tabla Probabilidad
Muy Baja	La actividad se realiza máximo 4 veces por año.	20%
Baja	La actividad se realiza mínimo 5 veces al año y máximo 12 veces al año.	40%
Moderada	La actividad se realiza mínimo 13 veces al año y máximo 365 veces al año.	60%
Alta	La actividad se realiza mínimo 365 veces al año y máximo 3660 veces al año.	80%
Muy Alta	La actividad se realiza 3661 veces o más al año	100%

Fuente: Curso Riesgo Operativo. Universidad del Rosario. 2020

Impacto

	Afectación Económica (o presupuestal)	Pérdida Reputacional
Insignificante 20%	Perdidas menores a 10 SMLMV .	Sólo de conocimiento de algunos servidores de la entidad.
Menor 40%	Mayores o iguales a 10 SMLMV y menores a 21 SMLMV	De conocimiento general de la entidad a nivel interno, de junta directiva y accionistas y/o de proveedores
Moderado- 60%	Mayores o iguales a 21 SMLMV y menores a 318 SMLMV	Afecta imagen con algunos usuarios que impacten significativamente los objetivos.
Mayor- 80%	Mayores o iguales a 318 SMLMV y menores a 2120 SMLMV	Deterioro de imagen con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayores a 2120 SMLMV	Deterioro de imagen a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Adaptado de Curso Riesgo Operativo. Universidad del Rosario. 2020

POLÍTICA INSTITUCIONAL
ADMINISTRACIÓN DEL RIESGO
UNIDADES TECNOLÓGICAS DE SANTANDER

LINEAMIENTOS PARA RIESGOS DE GESTIÓN

1.3. Valoración de Controles

Estructura para la descripción del control

- **Responsable de ejecutar el control**: Identifica el cargo del servidor que ejecuta el control, en caso se ser controles automáticos se identificará el sistema que realiza la actividad.
- **Acción**: Se determina mediante verbos en los cuales se identifica la acción a realizar como parte del control.
- **Complemento**: Corresponde a los detalles que permiten identificar claramente el objeto del control.

Eficiencia

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
Implementación	Automático	25%
	Manual	15%

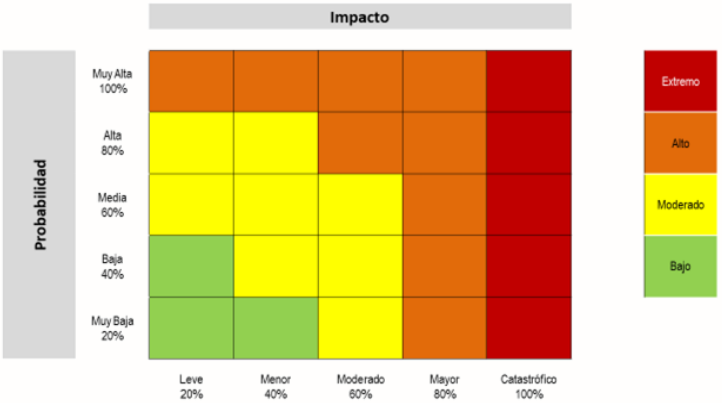
Atributos Informativos

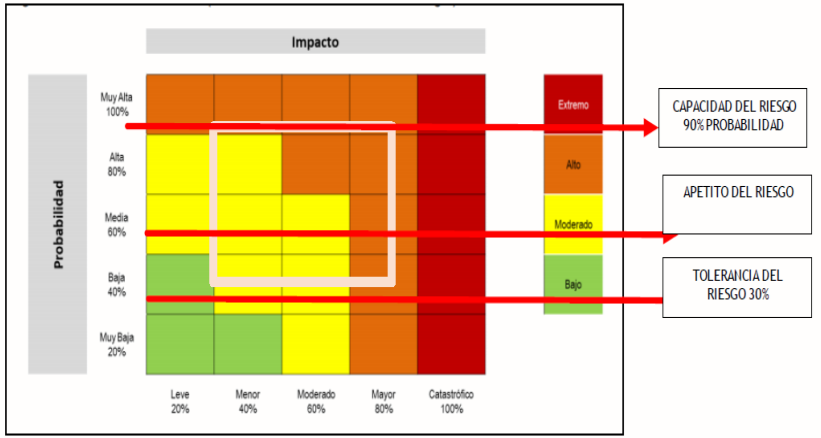
Formalización del Control	
Documentación	Documentado
	Sin Documentar
Frecuencia	Continua
	Aleatoria
Evidencia	Con Registro
	Sin registro

POLÍTICA INSTITUCIONAL
ADMINISTRACIÓN DEL RIESGO
UNIDADES TECNOLÓGICAS DE SANTANDER

LINEAMIENTOS PARA RIESGOS DE GESTIÓN

1.4. Evaluación de Riesgos





POLÍTICA INSTITUCIONAL
ADMINISTRACIÓN DEL RIESGO
UNIDADES TECNOLÓGICAS DE SANTANDER

LINEAMIENTOS PARA RIESGOS DE GESTIÓN

1.5. Estrategias para combatir el riesgo

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.

LINEAMIENTOS PARA RIESGOS DE GESTIÓN

1.6. Riesgos asociados a la continuidad de negocio

ESCENARIO	DESCRIPCIÓN
Emergencia Social	Agrupa todos los eventos asociados a la pérdida del orden público, pérdida de orden constitucional o situaciones en donde diversos actores generan acciones fuera del orden legal como: Asonada, revuelta civil, retención arbitraria de personal (secuestro).
Desastre natural y colapso de infraestructuras	Agrupa todos los fenómenos naturales o causados por el hombre que generan daño estructural del edificio y que obliga a evacuación del personal con el objetivo primario de salvaguardar la vida (incendio, sismo, inundación, falla de servicios eléctricos, hidráulicos, sanitarios)
Desastre Tecnológico	Falla de sistemas de información, pérdida de datos, fallas en sistemas de telecomunicaciones que interrumpen los procesos institucionales e inhabiliten el uso de servicios de tecnología de información y comunicaciones para el normal funcionamiento de la institución.
Financiero	Eventos que imposibilidad a la institución de contar con los recursos económicos para cumplir con compromisos misionales o con terceros como proveedores de servicios, estos eventos incluyen emergencia económica declarada por la rama ejecutiva, recortes presupuestales de emergencia o cambios económicos abruptos que desestabilizan el normal funcionamiento de la institución.
Sanitario	En esta categoría se agrupan los eventos causados por agentes biológicos que afectan a la salud de todos los seres vivos en particular la seguridad de los seres humanos, incluidos fenómenos como: pandemias, epidemias, crisis sanitaria que impide el funcionamiento de los procesos institucionales, entre otros.

POLÍTICA INSTITUCIONAL
ADMINISTRACIÓN DEL RIESGO
UNIDADES TECNOLÓGICAS DE SANTANDER

LINEAMIENTOS PARA RIESGOS DE GESTIÓN

1.7. Monitoreo y Revisión

RESPONSABLE	FRECUENCIA	REPORTE
COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO	Semestral	Pronunciamiento sobre el perfil de riesgo inherente y residual de la institución.
	Anual	Análisis de los riesgos institucionales.
	Semestral	Seguimiento sobre los riesgos ubicados en la zona de riesgos extremo.
PRIMERA LÍNEA DE DEFENSA LÍDERES DE PROCESOS Y SUS EQUIPOS DE TRABAJO	Cuatrimestral	Seguimiento a la implementación de los controles definidos y el plan de acción para los riesgos documentados en formato estandarizado.
SEGUNDA LÍNEA DE DEFENSA JEFE OFICINA DE PLANEACIÓN	Anual	Implementar la política institucional de administración del riesgo. Socializar la política institucional de administración del riesgo mediante circular, correos electrónicos, página web institucional, emisora, jornadas de inducción y reinducción institucional.
	Cuatrimestral	Monitorear el cumplimiento de las acciones contenidas en el mapa de riesgos de corrupción en el formato establecido para tal fin. Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos y realizar seguimiento a los planes de acción cuando el tratamiento del riesgo sea reducir (mitigar) Asesorar a los líderes de procesos respecto al tratamiento en los casos en que se materialice un riesgo.
TERCERA LÍNEA DE DEFENSA JEFE OFICINA DE CONTROL INTERNO	Cuatrimestral	Seguimiento a la gestión de riesgos de corrupción
	De conformidad con el Plan Anual de Auditoría	Seguimiento a los riesgos consolidados en los mapas de riesgos (F–CIG– 2 Lista Chequeo Actividades Gestión del Riesgo) y reportarlos los resultados al Comité Institucional de Coordinación de Control Interno CICC.

POLÍTICA INSTITUCIONAL

ADMINISTRACIÓN DEL RIESGO

UNIDADES TECNOLÓGICAS DE SANTANDER

LINEAMIENTOS RIESGOS DE CORRUPCIÓN

2.1. Disposiciones generales

2.2. Identificación del riesgo de corrupción

2.3. Valoración del riesgo

2.1. Disposiciones Generales

LINEAMIENTOS RIESGOS DE CORRUPCIÓN

2.2. Identificación del Riesgo de Corrupción

Las preguntas clave para la identificación del riesgo son:

- ¿Qué puede suceder?
- ¿Cómo puede suceder?
- ¿Cuándo puede suceder?
- ¿Qué consecuencias tendría su materialización?

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

POLÍTICA INSTITUCIONAL
ADMINISTRACIÓN DEL RIESGO
UNIDADES TECNOLÓGICAS DE SANTANDER

LINEAMIENTOS RIESGOS DE CORRUPCIÓN

2.3. Valoración del Riesgo

2.3.1. La determinación de la probabilidad

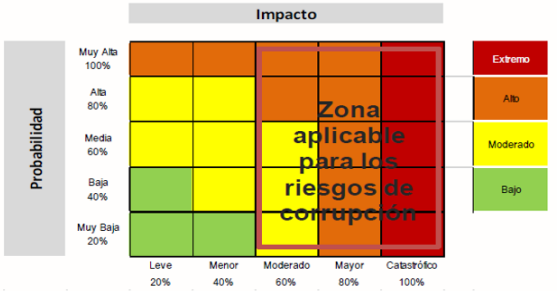
2.3.2. La determinación del impacto

2.3.3. Análisis preliminar (riesgo inherente)

2.3.4. Valoración de controles

No.	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA ...	RESPUESTA SI	RESPUESTA NO
1	¿Afecta al grupo de funcionarios del proceso?		
2	¿Afecta el cumplimiento de metas y objetivos de la dependencia		
3	¿Afecta el cumplimiento de la misión de la institución?		
4	¿Afecta el cumplimiento de la misión del sector al que pertenece la institución		
5	¿Genera pérdida de confianza de la institución, afectando su reputación?		
6	¿Genera pérdida de recursos económicos?		
7	¿Afecta la prestación de servicios?		
8	¿Da lugar al detrimento de la calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Genera pérdida de información de la institución?		
10	¿Genera intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Da lugar a procesos sancionatorios?		
12	¿Da lugar a procesos disciplinarios?		
13	¿Da lugar a procesos fiscales?		
14	¿Da lugar a procesos penales?		
15	¿Genera pérdida de credibilidad del sector?		
16	¿Ocasiona lesiones físicas o pérdida de vidas humanas?		
17	¿Afecta la imagen regional? (Nivel de Impacto: MAYOR)		
18	¿Afecta la imagen nacional?		
19	¿Genera daño ambiental		
Responder afirmativamente de UNA a CINCO preguntas(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico		10	
MODERADO	Genera medianas consecuencias sobre la institución		
MAYOR	Genera altas consecuencias sobre la institución		

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%



POLÍTICA INSTITUCIONAL
ADMINISTRACIÓN DEL RIESGO
UNIDADES TECNOLÓGICAS DE SANTANDER

LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

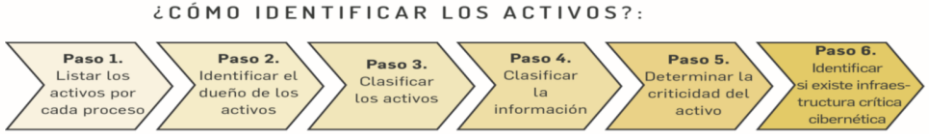
3.1. Identificación de los activos de seguridad de la información

3.2. Identificación del riesgo

3.3. Valoración del riesgo

3.4. Controles asociados a la seguridad de la información

3.1. Identificación de Activos de Seguridad de Información



¿QUÉ SON LOS ACTIVOS?	¿POR QUÉ IDENTIFICAR LOS ACTIVOS?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: Aplicaciones de la organización Servicios web Redes Información física o digital Tecnologías de información TI Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	Permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios). La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

3.2. Identificación del Riesgo

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Enlace Anexo 4: *Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas*
https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

POLÍTICA INSTITUCIONAL
ADMINISTRACIÓN DEL RIESGO
UNIDADES TECNOLÓGICAS DE SANTANDER

LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

3.3. Valoración del Riesgo

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

3.4. Valoración de Controles

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

¡Gracias!

uts Unidades Tecnológicas de Santander

¡Lo hacemos posible!