OFICINA DE POSTGRADOS

Tema:

APLICACIÓN DEL “NIST CYBERSECURITY FRAMEWORK” EN EL INSTITUTO SUPERIOR TECNOLÓGICO “SUCRE”.

Proyecto de Investigación y Desarrollo previo a la obtención del Título de Magíster en Ciberseguridad

Línea de Investigación:

Seguridad de la Información

Autor:

Ing. Jorge Alfredo Yánez Intriago

Director:

Mg. Galo Mauricio López Sevilla

Ambato - Ecuador

Junio 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

APLICACIÓN DEL "NIST CYBERSECURITY FRAMEWORK" EN EL INSTITUTO SUPERIOR TECNOLÓGICO "SUCRE"

Línea de Investigación:

Seguridad de la información

Autor:

Ing. Jorge Alfredo Yánez Intriago

Galo Mauricio López Sevilla Mg. f._____
CALIFICADOR

José Marcelo Balseca Manzano Mg. f._____
CALIFICADOR

Verónica Maribel Pailiacho Mena Mg. f._____
CALIFICADOR

Juan Carlos Acosta Teneda, P. PhD. f._____
DIRECTOR OFICINA DE POSTGRADOS

Pontificia Universidad Católica del Ecuador
OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villarroel. Dr. f._____
SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
SECRETARIA GENERAL
PROCURADURÍA

Ambato – Ecuador

Junio 2022

DECLARACIÓN Y AUTORIZACIÓN

Yo, Jorge Alfredo Yánez Intriago, portador de la cédula de ciudadanía Nro. 1001776283, autor del trabajo de graduación titulado: APLICACIÓN DEL "NIST CYBERSECURITY FRAMEWORK" EN EL INSTITUTO SUPERIOR TECNOLÓGICO "SUCRE", previa a la obtención del título profesional de Magíster en Ciberseguridad, en la oficina de Postgrados.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT, en formato digital, una copia del referido trabajo de graduación, para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad

Ambato, junio 2022

Jorge Alfredo Yánez Intriago
CC. 1001776283

AGRADECIMIENTO

En primer lugar, doy infinitamente gracias a Dios, por haberme dado fuerza y valor para culminar esta etapa de mi vida.

Agradezco, también, la confianza y el apoyo brindado por parte de mi madre y padre, que sin duda alguna en el trayecto de mi vida me han demostrado su amor, corrigiendo mis faltas y celebrando mis triunfos.

Al Ing. Galo López por toda la colaboración brindada, durante la elaboración de este proyecto.

Finalmente, a mi esposa e hijos porque cada uno con sus valiosas aportaciones hicieron posible este proyecto, por compartir momentos de alegría, tristeza y demostrarme su apoyo incondicional.

Jorge Alfredo Yánez Intriago.

DEDICATORIA

Dedico este trabajo principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional. A mi madre y padre, por ser el pilar más importante, por demostrarme siempre su cariño y apoyo incondicional. A mi familia en general, porque me han brindado su apoyo incondicional, por compartir momentos significativos conmigo y por siempre estar dispuestos ayudarme en cualquier momento. A mis profesores, gracias por su tiempo, por su apoyo, así como por la sabiduría que me transmitieron en el desarrollo de mi formación profesional.

Jorge Alfredo Yánez Intriago.

RESUMEN

El Instituto Superior Tecnológico Sucre no cuenta con mecanismos de ciberseguridad adecuados para proteger su plataforma tecnológica; al gestionar varios escenarios y plataformas, existe una alta probabilidad de que la ciberseguridad se vea afectada de manera negativa. En este contexto, es importante implementar contramedidas para que la institución identifique, proteja, detecte, responda y se recupere si se presenten incidentes de seguridad. Por lo tanto, el objetivo de este trabajo de investigación es aplicar el "NIST *Cybersecurity Framewor*k" con la finalidad de mejorar la postura de ciberseguridad en la organización. Este trabajo aporta con una investigación preexperimental de tipo longitudinal con enfoque cuantitativo. El "NIST *Cybersecurity Framework*" establece un proceso metodológico para que las organizaciones aseguren su plataforma tecnológica describe su postura actual de seguridad cibernética, establecer y evaluar el progreso hacia el objetivo deseado, identificar y priorizar oportunidades de mejora dentro del contexto de un proceso continuo y repetible; y, comunicar sobre los riesgos asociados a las partes interesadas internas y externas relevantes.Luego de la aplicación de este marco referencia se espera fortalecer el nivel de madurez de la ciberseguridad institucional a través del establecimiento y aplicación de un conjunto de mejores prácticas que permitan proteger la plataforma tecnológica más crítica.

Palabras claves: NIST, ciberseguridad, metodológico, madurez, seguridad.

ABSTRACT

The Higher Technological Institute “Sucre” does not have adequate cybersecurity mechanisms to protect its technological platform; by managing various scenarios and platforms, there is a high probability that cybersecurity will be negatively affected. In this context, it is important to implement countermeasures so that the institution identifies, protects, detects, responds and recovers when security incidents occur. Therefore, the objective of this research work is to apply the "NIST Cybersecurity Framework" in order to improve the cybersecurity posture in the organization. This will be a longitudinal pre-experimental work with a quantitative approach. The "NIST Cybersecurity Framework" establishes a methodological process for organizations to secure their technology platform by describing their current cybersecurity posture, establishing, and evaluating progress towards the desired goal, identifying and prioritizing opportunities for improvement within the context of a continuous process and repeatable; and, communicating about the associated risks to relevant internal and external stakeholders. After the application of this reference framework, it is expected to strengthen the level of maturity of institutional cybersecurity through the establishment and application of a set of best practices that allow protecting the most critical technological platform.

Keywords: NIST, cybersecurity, methodological, maturity, security.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

INTRODUCCIÓN

La pandemia provocada por COVID-19 en Latinoamérica a inicios del 2020, aceleró la transformación digital en todos los países por su fácil propagación a nivel mundial. La educación en todos los niveles se vio afectada con los cierres decretados en más de 200 países a nivel mundial, según el estudio de impacto elaborado por la UNESCO (2019) en que detalla recomendaciones para elaborar planes de contingencia para continuar los procesos educativos.

Según el estudio publicado por el Foro Económico Mundial (2020) en cuanto al impacto del COVID-19 en la educación a nivel mundial, indica que un total de 1.38 billones de estudiantes tuvieron que continuar su educación en modalidad virtual. Esto ocasionó que todas las instituciones de educación cambien su forma tradicional de brindar sus servicios educativos. Esta nueva realidad, también, afectó a los docentes que tuvieron que cambiar su forma tradicional de clases presenciales a virtuales, lo cual determinó nuevos retos de aprendizaje virtual para los educadores.

Con este nuevo escenario tecnológico, se presentaron vulnerabilidades explotadas por piratas cibernéticos. Por ello es importante que las instituciones de educación superior empiecen a crear estrategias para prevenir ataques cibernéticos en sus redes, datos, sistemas, entre otros. Según un estudio realizado por el medio de comunicación “El Economista” (2019) de la ciudad de México publicado el 26 de febrero de 2019, orientado al estudio de ciberataque por sectores, el sector educativo experimentó un incremento de ataques cibernéticos desde el inicio de la pandemia de un 6% a diferencia de otros sectores como el financiero en el cual, los ataques se incrementaron en un 19%, con ello es importante la necesidad de buenas prácticas en ciberseguridad en las instituciones de educación superior para gestionar los riesgos cibernéticos futuros, las vulnerabilidades siempre son explotadas por los ciberdelincuentes cada vez en una mejor forma.

Según la UNESCO (2021) un 70% de la población estudiantil se vio afectada por la pandemia, la misma que al experimentar una manera digital ocasionó una brecha que dejó a muchos estudiantes sin estudios por falta de elementos básicos tecnológicos en sus hogares. A nivel Latinoamérica no existen datos actualizados de la afectación de los ciberataques a instituciones de educación superior, tampoco cuáles medidas son tomadas como soporte para evitar nuevos ataques a sus organizaciones; Los estudios realizados en Ecuador sobre ciberseguridad y su aplicación en instituciones de educación son en forma general no se llega a un análisis concreto.

La educación superior evoluciona junto con la humanidad responde a la demanda de sus sociedades, por ello existen una gran cantidad de necesidades tecnológicas en las organizaciones en general; la comunidad universitaria tiene muchos retos tecnológicos, que permitan asegurar sus sistemas, redes y datos. Así la infraestructura de comunicación en las organizaciones de educación superior es susceptible a riesgos informáticos, al utilizar conexiones para intercambio de información, estos procesos son regulados para evitar pérdida por interceptación de datos durante el proceso de envío. A diferencia de Estados Unidos que cuenta con el Instituto Nacional de Estándares y Tecnologías por sus siglas en inglés NIST (2018), en Ecuador no existe un organismo que garantice el correcto manejo de información.

En el instituto Superior Tecnológico Sucre no existe una estrategia para el manejo de la ciberseguridad, en relación con la identificación, protección, detección, respuesta y recuperación de incidentes en seguridad informática. No es posible establecer un nivel de madurez organizacional en relación a Ciberseguridad que permita conocer el estado del instituto con relación a la seguridad informática por lo que es difícil establecer mejoras en ciberseguridad.

Con todo lo expuesto el problema planteado como pregunta es: ¿Cómo mitigar los riesgos cibernéticos en el Instituto Superior Tecnológico Sucre?

Para Proteger la plataforma tecnológica del Instituto Superior Tecnológico Sucre se realizó un análisis inicial de su estado en ciberseguridad, el cual comenzó con la revisión de su estado tecnológico a nivel de infraestructura, para determinar cada uno de los riesgos existentes y su nivel crítico.

Durante el proceso de estudio se determina que la Institución de Educación Superior (IES), no tiene un manejo adecuado de riesgos en ciberseguridad lo cual, le define como una institución vulnerable a posibles ataques en el ámbito de sus sistemas, redes y datos. Para la evaluación inicial se realizó una toma de información de los equipos de la institución, utilizar herramientas de diagnóstico para obtener información de sistemas operativos, hardware y redes de comunicaciones. Con los datos obtenidos se procedió a realizar un análisis previo para identificar el estado inicial de la institución.También, se revisó la infraestructura de su redes y manejo de su Centro de Procesamiento de datos para ver su estado en cuanto al manejo, configuraciones que se encuentran aplicadas dentro de la institución. La información obtenida permite determinar el estado de la institución y con ello obtener su nivel alcanzado.

Como reto y meta institucional para el 2022, la organización tiene un plan de mejoramiento continuo en su infraestructura tecnológica como lo determinaron en la rendición de cuentas del 2021 y está determinado en el anexo 2.

Para la búsqueda de la solución es necesario:

Objetivo General:
Aplicar el “NIST Cybersecurity Framework” para proteger la plataforma tecnológica del Instituto Superior Tecnológico Sucre.

Objetivos Específicos:

1. Definir la situación actual del estado del arte de las redes y datos del instituto Superior tecnológico Sucre.
2. Diagnosticar las principales falencias encontradas en la gestión de riesgos cibernéticos
3. Proponer contramedidas para gestionar los riesgos cibernéticos identificados
4. Elaborar una guía práctica de implementación de ciberseguridad para aplicar “NIST Cybersecurity Framework”.

La metodología que se implementa en este caso de estudio es la de NIST Framework la misma que está definida de la siguiente forma

- Describir la postura actual de ciberseguridad
- Describir el estado objetivo de ciberseguridad
- Identificar y priorizar oportunidades de mejora en el contexto de un proceso continuo y repetible
- Evaluar el progreso hacia el estado objetivo
- Comunicación entre las partes interesadas internas y externas sobre el riesgo de ciberseguridad

La aplicación del “NIST Cybersecurity Framework”, permite conocer el estado actual de la institución de educación superior que es el caso de estudio, partimos con realizar un análisis inicial para determinar un referente con el cual se generan las directrices necesarias para la correcta funcionalidad en todos sus sistemas, redes y datos para manejarlos bajo estándares a nivel internacional.

El “NIST Cybersecurity Framework”, permite a la institución tener una directriz necesaria para generar un plan de acción para mejoramiento continuo y finalmente, llegar a completar el perfil objetivo de la institución a nivel de seguridades en Ciberseguridad con la aplicación de los mejores estándares internacionales.

Al ser implementado el “NIST Cybersecurity Framework” por etapas se elabora un control dentro de cada uno de sus componentes como son los sistemas, redes y datos para cumplir con la normativa de acuerdo a estándares.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

Los Estados Unidos de América debido a la proliferación de vulnerabilidades y aumento de ataques cibernéticos considero necesario crear un ente regulador de políticas para el correcto funcionamiento de sus instituciones. Este organismo se denominó NIST (Instituto Nacional de Estándares y Tecnología), el cual fue fundado en marzo de 1901, que ha evolucionado con la tecnología y en la actualidad tiene como principal misión la innovación y la competencia industrial del país. El 12 de febrero de 2013, mediante orden ejecutiva del presidente Barack Obama se encargó al NIST el desarrollo del Marco de Ciberseguridad para la protección de infraestructuras críticas.

El marco de trabajo NIST (2018), desarrolla estándares de ciberseguridad, directrices, mejores prácticas y otros recursos para satisfacer las necesidades de la industria estadounidense, en su aplicación en organizaciones sudamericanas se demuestran casos exitosos como el de Uruguay, que son tomados como políticas de buenas prácticas.

Caso de estudio Universidad de Pittsburgh (*University of Pittsburgh*)

La Universidad *Pittsburgh* tiene su fundación en 1787, luego de dos devastadores incendios tuvo que cambiar de nombre y localización. Está compuesta por 17 facultades y su campus principal está situado en el barrio *Oakland* de *Pittsburgh*, del estado de Pensilvania, está situada en el puesto 80 de las mejores universidades del mundo y es líder en los campos de la medicina y filosofía. Uno de los grandes logros alcanzados por la universidad fue el descubrimiento de la primera vacuna para la polio en el año de 1955.

Es una universidad líder en los Estados Unidos en el área de investigación médica, previo a un análisis de ciberseguridad por el departamento de tecnologías de la información con sus siglas (TI) de la universidad adoptaron la implementación del

marco de ciberseguridad de NIST Universidad de *Pittsburgh* (2019), para cumplir con este proceso previa a una evaluación de los riesgos de la universidad se lo realizó en tres pasos:

Paso 1: Evaluación de riesgos en dos partes

Todos los departamentos universitarios completaron un cuestionario para la identificación de datos y determinar su confidencialidad.

Paso 2: Plan de mitigación

Se identificaron las mitigaciones existentes, se priorizo la gestión de riesgos, finalmente se trabajó y realizó un seguimiento de acciones de mitigación

Paso 3: Evaluaciones periódicas NIST 800-171 (2020)

Con la aplicación de NIST 800-171, la protección de la información no clasificada (CUI) permitió manejar una forma estandarizada para el cumplimiento de los requisitos de seguridad de TI descentralizado y volviéndolo ágil.

Como resultados e impactos se obtuvo un enfoque común simplificado de la documentación universitaria, existe una mayor conciencia y una visión más amplia en los riesgos de seguridad de la universidad, las unidades que no implementaron el marco de trabajo luego del éxito obtenido por los otros departamentos actualmente los están implementados.

A futuro la universidad provee estandarizar la evaluación de los riesgos como parte del procedimiento para el correcto uso de datos. Con el aumento de más departamentos con la aplicación del marco de trabajo, el departamento de TI tendrá un mejor seguimiento, identificación y respuesta de incidentes potenciales.

Caso de estudio Universidad de Chicago (*University of Chicago*)

Es una universidad privada creada en 1890 por John D. *Rockefeller*, su campus principal está ubicado en *Illinois* (Estados Unidos). Está situada entre las mejores del mundo y en los Estados Unidos está entre las más selectivas en el nivel educativo, desempeña un papel importante en el área de la investigación, como logros académicos tiene 101 premios Nobel. Al ser una universidad líder en el ámbito investigativo la División de Ciencias Biológicas por sus siglas (BSD) y manejar 23 departamentos.

El departamento de TI de la universidad de *Chicago* al reconocer las necesidades tecnológicas de los departamentos académicos, definió la necesidad de generar controles de seguridad para evitar duplicidad de esfuerzos en procesos mal estructurados. Con los antecedentes encontrados en seguridad de la información la institución educativa aplicó el proceso de implementación del marco de trabajo NIST BSD (2019), el mismo que estuvo distribuido en cuatro etapas:

Etapa 1: Revisión de las políticas y prácticas existentes para definir el estado actual en ciberseguridad por BSD.

Etapa 2: Evaluación de los riesgos de BSD en profundidad, con el estado encontrado se determinó el objetivo para el programa de ciberseguridad necesario.

Etapa 3: Se alinearon las políticas, procedimientos y prácticas en base a los riesgos encontrados en la Etapa 2.

Etapa 4: El equipo de implementación del marco de trabajo desarrolló una hoja de ruta priorizada describe las actividades necesarias de cumplimiento por los departamentos BSD para alcanzar el estado objetivo.

La implementación del marco de trabajo de Ciberseguridad de NIST fue exitoso, se desarrolló una herramienta de autoevaluación para ayudar a los departamentos a medir su progreso dentro de la hoja de ruta implementada. A futuro BSD alinea sus políticas de ciberseguridad existentes con el marco de trabajo para garantizar que el perfil de estado objetivo siga un proceso correcto.

De estos dos casos de estudio aplicados se determinó que NIST permite implementar un marco de trabajo que es adaptable al contexto de las organizaciones sin importar su tamaño e infraestructura con la finalidad de mejorar sus niveles de madurez de ciberseguridad, adicionalmente del análisis realizado a los dos casos de estudio se determinó que el marco de trabajo permite establecer estrategias para implementar y asegurar los activos digitales.

Las universidades de *Pittsburgh* y *Chicago* son tomadas como dos casos de éxito en la implementación del marco de trabajo NIST, las mismas que por su trayectoria en la formación de investigadores, en sus departamentos de TI buscaron la mejor opción de asegurar su información crítica para evitar las amenazas de ataque cibernéticos al ser información muy valiosa la que manejan sus respectivos departamentos. Con el análisis de estos dos casos de estudio de éxito a nivel de educación superior, se lo toma como referencia para su aplicación en el Instituto Superior Tecnológico Sucre.

1.1. Conceptos Generales

1.1.1. Ciberseguridad

Según Castillo y Bejarano (2020), la ciberseguridad no es más que una práctica correcta para defender las computadoras, los servidores, dispositivos móviles, las redes informáticas y los datos almacenados en cualquier gestor de base de datos que sufra ataques maliciosos. INCIBE, instituto Nacional de Ciberseguridad de

España (2017), define al término como prevenir, mitigar y dar una respuesta oportuna a los incidentes.

Con los antecedentes de los autores se determina que la ciberseguridad es la utilización de las mejores prácticas para prevenir, mitigar y dar una respuesta oportuna a los incidentes como disponibilidad de los aplicativos y el correcto acceso a los aplicativos webs, qué se presenten en una organización.

1.1.2. Ciberespacio

Está compuesto por redes de cómputo y telecomunicaciones que están interconectadas de manera directa o indirecta, por ello se determina que no solo lo conforma el internet, sino otros elementos lo cual, determina que es una zona de espacio con sus propias reglas. Lo indican Castillo y Bejarano (2020). Mientras que la Flacso, Facultad Latinoamericana de Ciencias Sociales (2017), determina que el ciberespacio es un dominio artificial construido por el hombre.

Analizar estos dos puntos de vista se deduce que el ciberespacio es una interconexión con un dominio artificial construido por el hombre que tiene sus propias reglas, y que su crecimiento en los últimos años es una preocupación para las naciones del mundo y cuerpos de seguridad ante las amenazas de organizaciones terroristas.

1.1.3. Ciberdefensa

Es prevenir y contrarrestar posibles incidentes o amenazas cibernéticas, en los últimos años la ciberseguridad y Ciberdefensa han tenido mayor interés político, con ello vuelven importante el correcto manejo de las TIC, en las organizaciones según Castillo y Bejarano (2020).

Por otro lado, la publicación de la Flacso (2017),determina que la Ciberdefensa es la protección de infraestructuras críticas con la especificación de programas de alerta.
Se toma estos dos conceptos se deduce que Ciberdefensa es la correcta protección de infraestructuras críticas para evitar posibles incidentes o amenazas y para su cumplimiento es necesario tener un correcto plan de protección de los mismos.

1.1.4. Activo de Información

Según el Instituto de Ciberseguridad de España INCIBE (2016) es cualquier recurso en una empresa necesario para el desempeño de sus actividades y cuyo fallo o deterioro ocasiona un agravio con costo económico, es necesario tener una correcta valoración de los activos para su evaluación de riesgo. Mientras que la norma ISO/IEC 27001 (2005) indica que un activo de información es algo que valora una organización y por lo tanto, estan protegidos.

Con estos dos conceptos se establece que un activo es cualquier bien informático necesario para el correcto funcionamiento organizacional y necesariamente estarían correctamente valorados para establecer su tipo de riesgo.

1.1.5. Amenazas

Para INCIBE (2016) es la circunstancia desfavorable que al ocurrir determina consecuencias negativas sobre los activos provoca su indisponibilidad. En la ISO 27001 (2005) determina que es toda cosa que al suceder, daña un activo de información, como desastres naturales, incendios o ataques de virus, espionaje.

Se concluye que una amenaza es ocasionada por cualquier circunstancia la cual, daña al activo de información y esto produce fallos dentro de su área de funcionamiento.

1.1.6. Vulnerabilidad

INCIBE (2016) indica que es una debilidad que presenta un activo y esta materializa las amenazas. Para la norma ISO 27001 (2005) son las debilidades propias de los activos que lo hacen susceptible de sufrir ataque o daños.
Una vulnerabilidad según las dos organizaciones es la debilidad que tienen los activos y por ello facilitan que se materialicen daños afecta su correcto funcionamiento produce que esta sufra daños.

1.1.7. Impacto

INCIBE (2018) define al impacto como la materialización de una amenaza sobre un activo aprovecha una vulnerabilidad. La ISO 27001 (2013), determina que un impacto es un coste para la empresa el mismo que va a generar un coste económico.

Con estas dos definiciones, se concluye que el impacto para una empresa está basado en un incidente previo al que se exponen los activos y estos van a ocasionar un costo económico para el negocio.

1.1.8 Valoración del impacto de un activo

La ISO 27001 (2013), determina que la valoración de un activo cuenta con una escala cuantitativa de 0 a 5, lo cual está determinado en la tabla 1, valoración de activos.

La Metodología de análisis y gestión de riesgos por sus siglas Magerit 3 (2012), valora los impactos de activos en una escala de 0 a 10 en su versión 3, lo cual está ilustrado en la tabla 2, valoración activos de Magerit 3.

Tabla 1. Valoración de Impactos ISO 27001

Impacto	Valoración
No Aplicable	0
Incidental	1
Menor	2
Moderado	3
Importante	4
Extremo	5

Fuente: tomado de la ISO 27001 (2013)

Tabla 2. Valoración Impactos por Magerit 3

Impacto	Valoración
Depreciable	0
Bajo	1 - 2
Medio	3 - 5
Alto	6 - 8
Muy alto	9
Extremo	10

Fuente: tomado de Magerit 3 (2012)

Con la revisión de las dos tablas de valoración manejan un total de impactos de seis valores, tiene su diferencia en la valoración cualitativa que es diferente en cada uno de los estándares.

1.1.9. Probabilidad.

La Norma ISO 27001 (2013), lo determina como la probabilidad para que un riesgo se materialice, para Magerit (2012), La probabilidad de amenaza de un activo está determinada por la ocurrencia de una amenaza y esta se disminuye si existen salvaguardias para su mitigación.

Tabla 3. Valoración Probabilidad ISO 27001 **(2013)**

Probabilidad	Valoración
Mínima	0
Baja	1
Media	2
Alta	3

Fuente: tomado de la ISO 27001 (2013)

Tabla 4. Valoración Probabilidad Magerit **(2012)**

Probabilidad	Valoración
Improbable	2
Posible	3
Probable	4
Casi certeza	5

Fuente: tomado de Magerit (2012)

Revisadas las dos tablas de probabilidad de la Norma ISO 27001 (2013), y Magerit (2012) manejan una valoración cuantitativa de cuatro valores y un estándar cualitativo, los dos estándares permiten manejar la gestión de la seguridad de la información de la mejor manera.

1.1.10. Medición de riesgos

La norma ISO 27001 (2013), determina que para calcular un riesgo es necesario partir de la probabilidad de ocurrencia del mismo. Mientras que en INCIBE (2018) dice que es una estimación de las ocurrencias y este se lo valora de una forma cuantitativa.

En estos dos conceptos, se determina que el nivel de un riesgo es el producto de un impacto por la probabilidad de su ocurrencia. En el gráfico 1 se evidencia la fórmula de medición de riesgos.

Gráfico 1: Fórmula para el cálculo de Riesgo

Fuente: tomado de INCIBE (2016)

1.1.11. Tratamiento de riesgos

En el tratamiento de riesgos esperado la empresa decide cuál es el mejor proceso que permita disminuirlo, para este cumplimiento es necesario tomar el costo económico para su remediación determinado por INCIBE (2016). La norma ISO 31000 (2018) determina que para el tratamiento del riesgo se determina seleccionar e implementar opciones para abordar los mismos.

Según INCIBE y la norma ISO 31000 (2018), el proceso de tratamiento de riesgo implica:

- Formular y seleccionar opciones para el tratamiento del riesgo
- Planificar e implementar el tratamiento del riesgo
- Evaluar la eficiencia de ese tratamiento
- Decidir si el riesgo residual es aceptable
- Si no es aceptable, efectuar tratamiento adicional

1.2. Gestión de Riesgos

Según Magerit (2012), para la correcta gestión de riesgos que implican dos grandes tareas a realizar:

- Análisis de riesgos
- Tratamiento de riesgos.
-

Mientras que NIST SP800-30 (2017), determina que la protección de la información de las organizaciones lleva un proceso lógico y analítico para cumplir con:

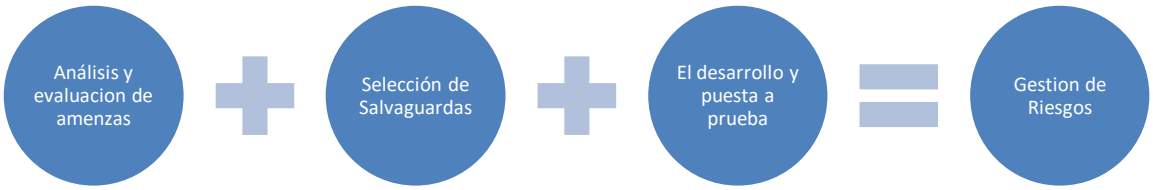
- El análisis y evaluación de amenazas
- La selección de salvaguardas para la mitigación de riesgos
- El desarrollo y puesta a prueba de planes de contingencia

Los dos estándares parten de un análisis y evaluación de riesgos para luego mediante el tratamiento de los riesgos crear un plan de contingencia para proteger la información de la organización. En los gráficos 2 y 3 se determina el proceso con cada uno de los estándares para la gestión de riesgos.

Gráfico 2. Gestión de riesgos con Magerit (2012)

Fuente: tomado de Magerit 3 (2012)

Gráfico 3. Gestión de Riesgos NIST 800-30 (2017)



Fuente: tomado de NIST 800-30 (2017)

1.3. Análisis del Riesgo

MAGERIT (2012) determina que un sistema de Información implica tener los controles necesarios para saber el estado real de seguridad de sus activos y permitan el correcto funcionamiento organizacional. Por otro lado, para NIST 800-30 (2017), establece el alcance y limitaciones operacionales para identificar defectos, amenazas, vulnerabilidades para analizar su impacto y con ello genera recomendaciones a la organización.

Los análisis de Riesgo para las dos metodologías determinan identificar para establecer controles para asegurar correctamente los activos que presentan vulnerabilidades para asegurarlos correctamente mediante controles adecuados.

1.3.1. Identificación de los Activos

Para la norma ISO 27001 (2013), la clasificación adecuada de activos de información está determinada por los tres pilares especificados de la información

- Confidencialidad
- Restringido
- Interno
- Público

De acuerdo con la Confidencialidad: La información es restringida y solo tiene acceso la alta dirección.De acuerdo con lo Restringido: Acceso válido para directores de área y empleados con este tipo de acceso.

De acuerdo con lo Interno: La información es accedida por los miembros de la organización en cualquier nivel. De acuerdo con lo Público: El acceso de la información es pública, dentro y fuera de la organización.

Según NIST 800-30 (2017), las principales amenazas de las organizaciones identifican en sus operaciones, activos o individuos y estas son internas o externas. Los dos estándares internacionales concuerdan en la identificación de activos con su probabilidad de ocurrencia como interno o externo y su afectación en la organización de acuerdo con su estado crítico.

1.3.2 Identificación de las amenazas

En cada organización una amenaza dependerá de su localización, entorno y actividad según los detalla la norma ISO 27001 (2013), MAGERIT (2012), determina que las amenazas afectan al activo y las clasifica en 4 tipos como lo detalla la tabla 5. Amenazas según MAGERIT.

Tabla 5. Tipos de amenazas según MAGERIT

Tipo de Amenaza	Descripción
[N] Desastres Naturales	Sucesos que ocurren sin intervención de los seres humanos como causa directa o indirecta.
[I] De origen industrial	Sucesos que ocurren de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas presentan de forma accidental o deliberada.
[E] Errores y fallos no intencionados	Fallos no intencionales causados por las personas.
[A] Ataques intencionados	Fallos deliberados causados por las personas.

Fuente: tomado de Tipo amenazas MAGERIT (2012)

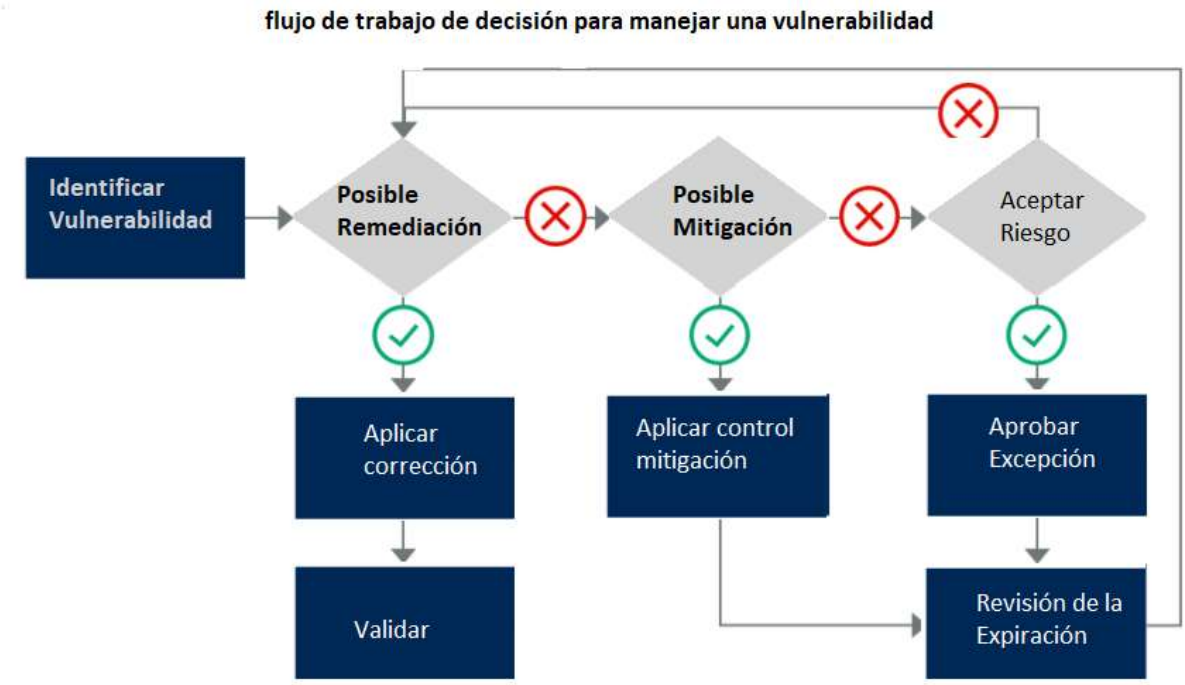
1.3.3. Identificación de vulnerabilidades

La metodología NIST (800-30) determina como identificación de vulnerabilidades a un listado de defectos o debilidades que nos permite conocer las posibles intrusiones de una amenaza.

Según la norma ISO (27001 I.),existe un evaluación cuantitativa o cualitativa de riesgos asociados a vulnerabilidades los mismos que parte de una amenaza a un activo.

Los dos estándares determinan la importancia de encontrar las principales vulnerabilidades que se asocian a las amenazas de los activos. En el gráfico 4 se determina el flujo de trabajo para identificar una vulnerabilidad según Gartner.

Gráfico 4. Identificación de Vulnerabilidad



Fuente: tomado de Gartner Id:410271

1.3.4. Identificación de la existencia de controles

Se elabora un listado de controles existentes en la organización de existir si no se elabora una lista de los controles necesarios como lo establece la metodología de NIST (2017). Según la ISO (27001 I.),es necesario definir las reglas y restricciones por medio de políticas organizaciones para normar el correcto manejo de los procesos en cada una de las áreas que manejan activos según un análisis de riesgos.

Las dos normativas concuerdan en la necesidad de controles dentro de una organización para manejar los riesgos potenciales de mejor manera y tener una adecuada respuesta.

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la organización

El instituto Superior Tecnológico Sucre es una entidad de educación superior con sede en la ciudad de Quito, su origen se remonta al año 1959, si se fundó el colegio Técnico Nacional Sucre. En julio 17 de 1996, la Dirección Nacional de Planeamiento de la Educación, lo eleva a la categoría de Instituto Tecnológico Superior con el acuerdo N.- 4191, con las especialidades de Electricidad y Electrónica Industrial. Cuatro años después, el Consejo Nacional de Educación Superior con sus siglas (CONESUP) mediante registro institucional N.- 17-024, le otorga el nivel de Instituto Tecnológico Superior Sucre. A partir del año 2019, con reforma al artículo 118 de la Ley Orgánica de Educación Superior (LOES) otorga títulos de tercer nivel académico. El 15 de febrero del 2019, mediante comunicado RPC-SO-04-No. -057-2019. La Secretaría de Educación Superior y Tecnología (SENESCYT), de acuerdo a las disposiciones transitorias Sexta y Tercera del Reglamento de las Instituciones de Educación Superior de Formación Técnica y Tecnológica realiza un cambio en la denominación del instituto como Instituto Superior Tecnológico Sucre.

Misión Institucional

Formamos profesionales competentes con espíritu emprendedor, capaces de contribuir al desarrollo integral del país, tomado de rendición de cuentas (2020).

Visión Institucional

Ser una Institución Superior Universitaria con estándares de calidad académica e innovación, reconocida a nivel nacional con proyección internacional, tomado de la rendición de cuentas (2020) .

En la actualidad la Institución de Educación Superior (IES), oferta un total de 10 carreras a nivel Superior Tecnológico, la misma que se detalla en el gráfico 5 de estudiante matriculados por carreras en el año (2020) tomado de la rendición de cuentas de la institución en ese año.

Gráfico 5: Estudiante matriculados 2020 por carreras

CARRERA	NÚMERO DE ESTUDIANTES MATRICULADOS 2020		
	2020 I	2020 II	TOTAL 2020
CONTABILIDAD	50	237	287
DESARROLLO DE SOFTWARE	128	205	333
ELECTRICIDAD	263	283	546
ELECTROMECÁNICA	232	301	533
ELECTRÓNICA	252	292	544
GESTIÓN AMBIENTAL	314	441	755
MARKETING	161	354	515
PRODUCCIÓN Y REALIZACIÓN AUDIOVISUAL	126	213	339
DESARROLLO INFANTIL INTEGRAL	174	160	334
PRODUCCIÓN TEXTIL	69	79	148

Fuente: tomado de rendición de cuentas ITS SUCRE (2020)

2.1.1. Organigrama Institucional

El organigrama institucional está determinado por el Anexo 3, donde se detalla el orden jerárquico estructural determinado por la institución En la actualidad cuenta con una planta estudiantil de 2300, estudiantes que se encuentran distribuidos en las 10 carreras ofrecidas por la institución, para cumplir con su noble labor cuenta con dos sedes norte y sur, la mismas que están distribuidas para una correcta formación estudiantil.

El crecimiento a carreras nuevas y cantidad de estudiantes determina un crecimiento en cuanto a necesidades tecnológicas que pone al departamento de TICS de la institución tomar el correcto manejo de sus seguridades en cuanto a sistemas, redes y datos. Por ello se presenta como una necesidad institucional la implementación del marco de ciberseguridad para verificar su situación inicial y con ello determinar un correcto manejo en cada uno de los elementos analizados para determinar el nivel de implementación del marco de trabajo NIST en la institución. Con ello se cumple el primer objetivo estratégico institucional que evidencia “Incrementar los estándares de calidad Institucional”, rendición de cuentas (2020).

2.1.2. Objetivos

- Incrementar los estándares de calidad Institucional
- Alcanzar la excelencia académica, organizacional y tecnológica que permita la condición de Instituto Superior Universitario
- Afianzar la institución a nivel nacional con proyección internacional.

Sobre la base del análisis realizado a la Organización, el “NIST” se ha implementado en los servicios críticos de la unidad de tecnologías de la información y comunicación.

2.2. Metodología de investigación

2.2.1. Tipo de Investigación

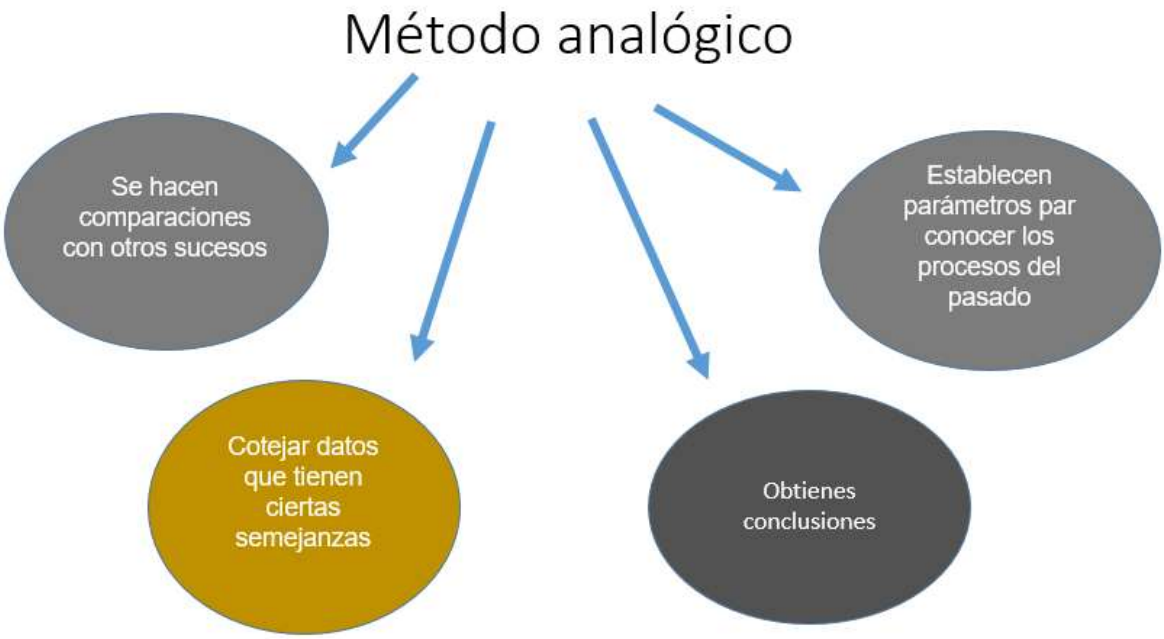
La investigación para aplicación en la implementación de marco de trabajo de NIST, fue cuantitativa en el proceso de aplicación de las listas de chequeo tanto para el estado actual como para el objetivo deseado y con una valoración cualitativa para determinar las prioridades altas que son las aplicadas en el plan de acción institucional según el nivel alcanzado por cada una de las subcategorías de listas de verificación de aplicación para el conocimiento del estado actual en la institución Educativa.

2.2.2. Métodos

El método de investigación analógico es el que se utilizó en la presente investigación al tener la comparativa de un estado actual con un objetivo deseado para la determinación de la brecha obtenida.

Según el documento publicado por la Universidad Autónoma de Chiapas (2017), el método analógico permite realizar comparaciones de sucesos para cotejar datos obtiene ciertas semejanzas si existen y con ello llegar a conclusiones. En el gráfico 7, se determina el proceso que se cumplió en la aplicación de las fases de implementación del marco de trabajo de NIST.

Gráfico 6: Método Analógico.



Fuente: tomado de la Universidad Autónoma de Chiapas, México (2017)

2.2.3. Técnicas y Herramientas

Técnica de recolección de Información: Para la recolección de información se utilizó la encuesta ver Anexo 1. Los resultados obtenidos luego de la aplicación de la encuesta para identificar los riesgos emergentes institucionales son los mismos que se detallan a continuación.

En el Anexo 2 Pregunta 1, se determina que el departamento Académico cuenta con la mayor cantidad de usuarios ocupa en la institución con 54%, según el gráfico obtenido, luego está el departamento de tecnologías de la información con un 10%, Titulación 8%, Dirección Administrativa 7%, Bienestar Estudiantil 5%, Formación Integral 5%, Aseguramiento de la Calidad 5%, finalmente Investigación y Desarrollo 3%, Coordinación estratégica con un 3%.

Pregunta 2 Existen elementos críticos asignados a su departamento (Ejemplo Sistemas Informáticos, redes de computadoras, Almacenamiento de información). En el anexo 2 se determina el gráfico de resultado obtenido con un 80% para el departamento de Tecnologías de la Información y un 20% de Otros departamentos.

Pregunta 3 Maneja algún sistema (Ejemplo Sistema Académico, Aulas Virtuales, Sistema Gestión Documental). El resultado obtenido fue de 90% para el Departamento de Tecnologías de la Información y 10% para Otros departamentos como está en el gráfico del anexo 2.

Pregunta 4 Utiliza Información Crítica (Ejemplo Administración de Bases de Datos Institucionales). En esta pregunta el resultado obtenido es de 95% de manejo de Información crítica para el departamento de Tecnologías de la Información y un 5% para los otros Departamentos. En el anexo 2 se encuentra el gráfico resultante de la encuesta realizada.

Pregunta 5 Usa algún tipo de respaldo de información (Ejemplo Disco externos, Datos en la Nube). El departamento de Tecnologías de la Información tiene un 60% del uso de respaldo frente a un 40% de otros Departamento, esto se encuentra en el anexo 2, como resultado de la encuesta.

Pregunta 6 Maneja base de datos institucionales (Ejemplo Ingreso, actualización, eliminación de información de sistemas). En el anexo 2 se registra con un 98% al departamento de Tecnologías de la Información frente a un 2% de otros Departamentos en cuanto al manejo de base de datos institucionales.

Pregunta 7 Maneja interconexiones institucionales (Ejemplo administra una red de datos departamental), Como resultado de esta pregunta se obtuvo un 100% como manejo de las redes institucionales para el departamento de Tecnologías de la información. Ver anexo 2 resultado de pregunta 7.

Pregunta 8 Alguno de los equipos de su departamento permiten la correcta funcionalidad institucional (Ejemplo Servidor o equipo de manejo de respaldos). El resultado obtenido en la encuesta aplicada en esta pregunta consta en el anexo 2, el Departamento de Tecnologías de la información tiene el 95% de los equipos críticos de la organización y el otro 5% está en los restantes Departamentos encuestados.

Pregunta 9 El correcto funcionamiento de su departamento depende de la correcta disponibilidad de aplicaciones. En esta pregunta debido a la criticidad de la información es el Departamento de Tecnologías de la Información con un 95% el responsable de la disponibilidad de todas las aplicaciones institucionales y un 5% de otros departamentos con información externa requerida. Esto se evidencia en el anexo 2.

Pregunta 10 Tiene conocimientos básicos de los riesgos informáticos existentes. Todos los departamentos encuestados evidencian tener conocimientos básicos sobre los principales riesgos informáticos existentes conocidos, Tecnologías de la Información con un 60% y los otros departamentos con un 40%, ver anexo 2 gráfico resultante.

En la tabla 6. Se define el resultado de la aplicación de la encuesta institucional realizada a 8 unidades que se tomaron como las más relevantes para la aplicación de la encuesta después de un análisis de procesos de las actividades institucionales. De estos el departamento de Tecnologías de la Información es la unidad más crítica de la institución al manejar los activos informáticos vitales para el correcto funcionamiento de la organización.

Tabla 6. Resultado de Encuesta Selección unidad Crítica ITS SUCRE

Unidades Evaluadas	Año de Evaluación	Total, Preguntas	Porcentaje de unidades Críticas encontradas	Unidad que tiene el mayor porcentaje de activos críticos
8	2021	10	1	1

Fuente: elaboración propia aplicación encuesta ITS SUCRE

Las Unidades seleccionadas para ser evaluadas son:

Aseguramiento de la Calidad

Coordinación estratégica

Tecnologías de la Información y comunicación

Bienestar institucional

Investigación y Desarrollo

Dirección administrativa

Formación Integral

Titulación

Las preguntas evaluadas están determinadas en el Anexo 1. Las mismas que determinaron como resultado los porcentajes alcanzados por análisis de manejo de elementos críticos institucionales como lo detalla la Tabla 7.

Tabla 7: Detalle resultados encuesta ITS SUCRE

Unidad de Aplicación	% Pregunta 1	% Pregunta 2	% Pregunta 3	% Pregunta 4	% Pregunta 5	% Pregunta 6	% Pregunta 7	% Pregunta 8	% Pregunta 9	% Pregunta 10	% total
Aseguramiento de la Calidad	2	1	1	1	3	1	0	1	1	6	1,6
Coordinación estratégica	2	2	2	1	4	1	0	1	1	8	2,2
Tecnologías de la Información y comunicación	80	80	90	95	60	98	100	95	95	60	85,3
Bienestar institucional	8	6	1	0	8	0	0	1	1	3	2,8
Investigación y Desarrollo	2	3	2	1	8	0	0	1	2	6	2,5
Dirección administrativa	2	4	1	0	9	0	0	1	0	5	2,2
Formación Integral	3	2	2	1	4	0	0	0	0	8	2,0
Titulación	1	2	1	1	4	0	0	0	0	4	1,3

Fuente: elaboración propia aplicación encuesta ITS SUCRE

2.3. Metodología de desarrollo

2.3.1. Identificar los requerimientos regulatorios para el alcance en el ITS SUCRE

En la tabla 8. se determinan los requerimientos legales, que manejan la siguiente información:

Requisito: Información artículo según Reglamento institucional ITS SUCRE

Documento que impone el requisito: Detalle reglamento Interno del ITS SUCRE según el requisito

Persona responsable del cumplimiento: A quién va dirigido para cumplimiento el requisito Según el reglamento Interno del ITS SUCRE

Plazos: Si tiene un plazo definido para su cumplimiento según el reglamento interno ITS SUCRE.

Partes interesadas: Descripción de aplicación del reglamento o ley, departamentos a los que se dirige su cumplimiento.

Tabla 8: Tabla de Requerimientos Legales

Requisito	Documento que impone el requisito	Persona responsable del cumplimiento	Plazos	Partes interesadas
Artículo 31.- Ambientes y medios de estudio o aprendizaje. - Las tutorías se efectúan en distintos ambientes académicos, laborales, simulados y/o virtuales, además, de diversas formas de interacción entre docentes y estudiantes. Para su desarrollo, promueve la convergencia de medios educativos y el uso adecuado de tecnologías de información y comunicación (TICs).	REGLAMENTO INTERNO DE RÉGIMEN ACADÉMICO DEL INSTITUTO SUPERIOR UNIVERSITARIO SUCRE	Comunidad académica	No aplica	Docentes Estudiantes Autoridades
Artículo 56.- Modalidades de estudio. - Las modalidades de estudio o	REGLAMENTO INTERNO DE	Comunidad académica	No aplica	Docentes Estudiantes Autoridades

aprendizaje son modos de gestión de los aprendizajes que determinan ambientes educativos diferenciados, incluye el uso de las tecnologías de la comunicación y de la información.	RÉGIMEN ACADÉMICO DEL INSTITUTO SUPERIOR UNIVERSITARIO SUCRE			
Artículo 59.- Modalidad híbrida.- La modalidad híbrida es aquella en la que los componentes de aprendizaje en contacto con el docente, práctico-experimental, y aprendizaje autónomo de la totalidad de las horas o créditos, se desarrollan mediante la combinación de actividades presenciales, semipresenciales, en línea y/o a distancia; usa para ello recursos didácticos físicos y digitales, tecnologías interactivas multimedia y entornos virtuales de aprendizaje, que organizan la interacción de los actores del proceso educativo, de forma sincrónica o asincrónica, a través de plataformas digitales.	REGLAMENTO INTERNO DE RÉGIMEN ACADÉMICO DEL INSTITUTO SUPERIOR UNIVERSITARIO SUCRE	Comunidad académica	No aplica	Docentes Estudiantes Autoridades
Artículo 88.- Procedimiento para modificación de registro de calificaciones y/o asistencias. - El docente solicita a la coordinación de carrera en un término de hasta 30 días, posteriores a la fecha fijada en el cronograma general de actividades académicas para el ingreso de una	REGLAMENTO INTERNO DE RÉGIMEN ACADÉMICO DEL INSTITUTO SUPERIOR UNIVERSITARIO SUCRE	Comunidad académica	No aplica	Docentes Estudiantes Autoridades

calificación o asistencia al sistema académico, que por errores manifiesto o recalificación de alguno de los medios de evaluación, existan modificaciones o cambios; establece la debida justificación motivada. La coordinación entrega un oficio con la respuesta a la solicitud del docente, para que desde secretaria de carrera gestiona el cambio de nota en el sistema, de manera conjunta con soporte de tecnologías de la información de la carrera, debido a la restricción que cuenta el docente para realizar el cambio desde su usuario en el sistema SAGA.				

Fuente: elaboración a partir Reglamento interno ITS SUCRE

Para cumplir con la implementación de NIST en el Instituto Superior Tecnológico se implementa su orden metodológico definido en las siete etapas para cumplir con el objetivo final que es la implementación del marco de trabajo. En el gráfico 7 se determinan los componentes del marco básico de trabajo.

Gráfico 7: Marco básico trabajo NIST

Fuente: tomado a partir de NIST (2018)

El Marco de trabajo de NIST, está compuesto por el núcleo, niveles y perfiles los mismos que en conjunto permiten mitigar los riesgos de ciberseguridad de la organización a ser implementada.

Núcleo (*Core*): Son los resultados deseados organizados por jerarquía y alineados con guías y controles detallados. Nivel Implementación (*Tires*): Es una medición cualitativa en prácticas de la organización en gestión de riesgos de ciberseguridad. Perfil (*Profile*): Es la alineación en cuanto a requisitos y objetivos de la organización para la obtención de resultados deseados luego de su proceso de implementación.

Para su correcta funcionalidad el marco de trabajo de NIST, consta de un núcleo (*CORE*), que tiene cinco funciones, 23 categorías y 108 subcategorías las cuales, están distribuidas entre cada una de las funciones para obtener los resultados basados en riesgos que se adaptan a las necesidades de la organización.

2.3.2. Identificar (*Identify*)

Es la primera función del marco de trabajo de NIST, en la que se detalla una comprensión de la gestión de riesgos asociados a los sistemas, datos y capacidades de su infraestructura crítica. En la ISO 27001 (2013), determina que la principal función del análisis de riesgos es la identificación de activos, amenazas y vulnerabilidades.

Los dos estándares concuerdan con la importancia de partir con la identificación de riesgos para perder cumplir con el proceso de implementación de una metodología para gestionar y minimizar amenazas en las organizaciones. Para el cumplimiento de esta función la NIST implementa las siguientes categorías:

1. Gestión de activos (ID.AM):
2. En esta categoría del marco de trabajo se realizó la identificación de sistemas, dispositivos, usuarios, datos e instalaciones, se los clasificó de acuerdo a importancia crítica. Los detalles de activos encontrados en la institución se detallan en la tabla 9, el detalle de la tabla está definida de la siguiente formaIdentificador: Referencia al código interno manejado por la institucionNombre: Se refiere al nombre físico del equipo definido como activoDescripción: Una breve descripción de las características del activo encontrado en el inventario institucional.Responsable: Es el integrante del equipo responsable que se encarga de la custodia del activo de información.

Modelo: Modelo del fabricante del equipo, detalla las características principales del activo de información encontrado.

Tipo: Está basado en el estándar de MAGERIT 3.0 (2012), tipos de activos.

Ubicación: Define la ubicación física del activo. Por el estado de criticidad del activo sólo se brinda una referencia mas no su ubicación específica.

Tabla 9: Inventario de Activos Instituto Superior Tecnológico Sucre

IDENTIFICADOR	NOMBRE	DESCRIPCIÓN	RESPONSABLE	MODELO	TIPO	UBICACIÓN
ID_001	SERVIDOR UIO	SERVIDOR PRINCIPAL WEB Y DE BASE DE DATOS	GERENTE DE TI JEFE DE INFRAESTRUCTURA	HP PROLIANT	[HOST] Grandes Equipos	CENTRO DE DATOS (Matriz)
ID_002	ROUTER	ROUTER RED INALÁMBRICA ÁREA ADMINISTRATIVA	GERENTE TI	CISCO 800	[router] encaminadores	CENTRO DE DATOS(Matriz)
ID_003	SWITCH	RED CABLEADA LABORATORIO 301	GERENTE TI	DLINK	[switch] conmutadores	LABORATORIO 301 MATRIZ PRINCIPAL
ID_004	ROUTER WIRELESS	RED DOCENTES EDIFICIO MATRIZ	GERENTE TI	DLINK	[router] encaminadores	EDIFICIO MATRIZ UIO
ID_005	RACK DE PARED	ÁREA DE SERVIDORES UIO	GERENTE TI	3M	[network] soporte de la red	CENTRO DE DATOS(Matriz)
ID_006	UPS APC	ÁREA DE SERVIDORES UIO	GERENTE TI	APC	[ups] sistemas de alimentación ininterrumpida	CENTRO DE DATOS(Matriz)
ID_007	SISTEMA WINDOWS 10	LABORATORIOS	GERENTE TI	20 PC	[pc] informática personal	LABORATORIO 310
ID_007	CERRADURA ELÉCTRICA	AREA DE SERVIDORES	GERENTE TI	S/M	[electronic] electrónicos	CENTRO DE DATOS(Matriz)

Fuente: elaboración propia inventario TICS ITS SUCRE.

3. Entorno empresarial (ID.BE):

En base a la misión de la Institución, objetivos, procesos se crearon los roles, responsabilidades para la toma de decisiones en seguridad de acuerdo a las distintas áreas críticas. Se realiza el análisis de funciones y responsabilidades para cumplir con NIST 800-55 (2020), pero no se tiene una asignación y se toma como referente para la aplicación del checklist como un requerimiento para el correcto cumplimiento del proceso del marco de trabajo.

Funciones y responsabilidades básicas requeridas Jefe de Organización: El mismo que garantiza el apoyo de planificación estratégica, apoya al CIO para el correcto cumplimiento según sus informes anuales. Director de Información (CIO): Permite mantener monitoreado los sistemas y datos para su correcto funcionamiento, adicionalmente aplica las medidas de seguridad de información requeridas en la organización.

Oficial principal de seguridad de la información (CISO): Es el encargado del desarrollo e implementación de programas de seguridad de la información, si considera necesaria asignación de recursos solicitarlo para agendarlo en el plan anual elaborado por el CIO.
Otros roles: Según el análisis y requerimiento por el CIO en su informe anual, se determina según el crecimiento de la organización la creación de nuevos roles.

4. Gobernanza (ID.GV): Se aplican las políticas y procedimientos para la correcta administración de los requisitos regulatorios de acuerdo al marco de trabajo de NIST. Se revisa las políticas existentes en la organización y se detalla que no están correctamente reglamentadas por ello se lo marca en el checklist como una necesidad y se detalla las políticas básicas requeridas, ver gráfico 16.

Administración de Cuentas: Se determina la necesidad de tener una política de tipos de cuentas y sus perfiles para el correcto uso de cada una de los sistemas implementados.

Gestión de Cuentas: Existe una política que determine el proceso para la creación, habilitación, modificación, des habilitación y eliminación de cuentas. Para las cuentas deshabilitadas, crea una política que determine cómo se realiza el proceso para su correcta aplicación.

Los usuarios reciben capacitaciones permanentes de buenas prácticas para el uso correcto de credenciales y que los sistemas manejan métodos de autenticación con control de sesión para evitar fallos de seguridad al quedar por error de un usuario un aplicativo abierto. No se encontró una política de acuerdo de confidencialidad para el buen uso de los aplicativos institucionales.

5. Evaluación de riesgos (ID.RA): Con la comprensión de los riesgos de ciberseguridad que generan afectaciones a la organización, las partes encargadas de la seguridad de la información garantiza la correcta funcionalidad de las operaciones diarias.¡ Para el proceso de evaluación de riesgos se aplicó Cobit 5 (2019), en sus procesos de gestión según el *framework* de la Asociación de Control y Auditoría de Sistemas de Información con sus siglas (ISACA), es importante tomar en cuenta los siguientes elementos:

- Contar con personal suficiente para el desarrollo del proceso de gestión de riesgos.
- Estar seleccionado el personal clave de TI en la organización.
- Tener una planificación del uso de recursos en la organización.

- Cumplir con las metas y objetivos organizacionales para su correcto funcionamiento. Las metas y objetivos organizacionales están determinados en la tabla 8, del reglamento interno de la institución, como lo determina Cobit 5.

6. Estrategia de gestión de riesgos (ID.RM): Se determinan las prioridades, restricciones, para el correcto manejo de riesgos operacionales de la organización. Los riesgos están determinados de acuerdo a los activos evidenciados en la tabla 3, se clasifican de acuerdo a la criticidad.

En la organización no se detectaron actores para el cumplimiento de la gestión de riesgos detallados, con ello se evidencia la necesidad de fomentar una política de análisis de riesgos para solventar las deficiencias encontradas en el análisis inicial realizado.

7. Gestión de riesgos de la cadena de suministro (ID.SC): Se establecen las prioridades para la tolerancia en riesgos dentro de la institución. Para el cumplimiento la organización determina los productos necesarios para la mitigación de riesgos. Ver en la tabla 9.

Es necesario que en la organización, se fomente un correcto proceso de manejo de riesgos en cada uno de los procesos que manejan sus sistemas implementados para cumplir con la priorización de los riesgos cibernéticos que se encontraron en la fase inicial.

2.3.3. Proteger (*Protect*):

Permite reforzar las protecciones de seguridad de la información con la finalidad de salvaguardar sus activos críticos. Para el cumplimiento maneja cinco categorías:

1. Gestión de Identidades, Autenticación y Control de Acceso (PR.AC):

Es necesario limitar el acceso a los activos físicos y lógicos de la organización según el riesgo evaluado de acceso. Los accesos a las redes institucionales cuentan con una clave general y no están segmentadas por departamentos, lo cual es un riesgo informado.

Las codificaciones para el acceso a los aplicativos webs utilizan una encriptación con estándares mínimos para su correcto funcionamiento.

No se detectó una política de correcta gestión de cuentas como lo detalla NIST 800-171 (2020), como se detalla a continuación

- Creación
- Modificación
- Habilitación
- Inhabilitación
- Remoción

2. Sensibilización y Formación (PR.AT): Se determina si la organización capacita al personal y socios de la organización en ciberseguridad, determina sus deberes y responsabilidades en cuanto a seguridad de la información. Ver tabla 19 de resultados aplicación.

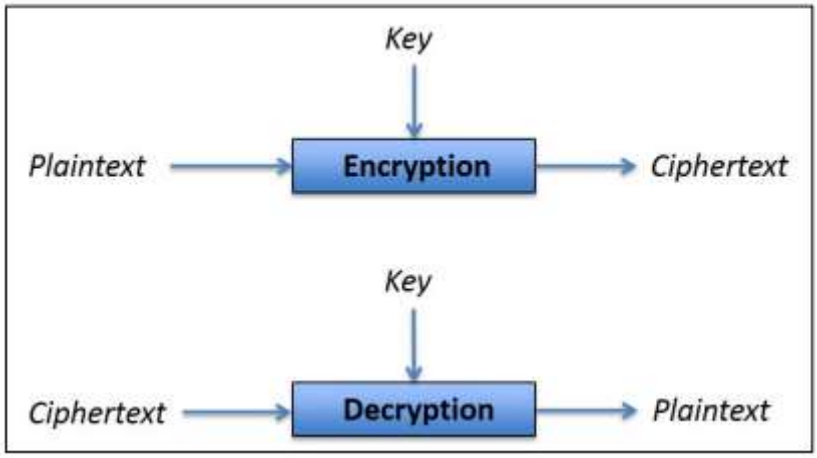
No existe un conocimiento de las jerarquías para el proceso de control y manejo ciberseguridad en la institución, la autoridad mayor no tiene conocimiento del rol dentro del proceso de ciberseguridad en la organización y de la necesidad de la asignación de personal de TI para el correcto funcionamiento del control de gestión de riesgos.

Tampoco se evidencia la existencia de un plan de capacitación al personal para el correcto manejo de los aplicativos y de la importancia de la seguridad de la información dentro de la organización.

3. Seguridad de los Datos (PR.DS): La organización administra la información y los registros de acuerdo con la estrategia de riesgo de la organización para lograr proteger la confidencialidad, integridad y disponibilidad de la información.

No se detectó un correcto manejo de información encriptada como lo detalla NIST 800-175 (2020), en la cual, maneja una llave en inglés (*Key*) junto a un código de cifrado como el de los estándares avanzados de cifrado por sus siglas en inglés (*AES*) como lo detalla el gráfico 8. Según la aplicación del checklist de NIST del estado actual en la categoría de Procesos y procedimientos de la información.

ráfico 8: Modelo encriptación AES



Fuente: tomado a partir de NIST 800-175 (2020).

4. Procesos y Procedimientos de Protección de la Información (PR.IP):

La administración de la protección de los sistemas y activos de información, se establecen de acuerdo a los procesos y procedimientos.

Según la ISO 27001 (2013), es necesario definir los riesgos asociados, controles del riesgo, como requisitos básicos para la seguridad de la información. También, nos indica la necesidad de la seguridad en los procesos de desarrollo y soporte de sistemas de información.

5. Tecnología de protección (PR.PT):

Se garantizan soluciones técnicas de seguridad de acuerdo a las políticas, procedimientos institucionales en cuanto a sistemas y activos.

En la tabla 10, se detalla las mayores amenazas presentadas a las redes inalámbricas y de datos que están protegidas según la publicación de NIST 800-48 (2018).

Tabla 10: Principales amenazas contra la seguridad de la red

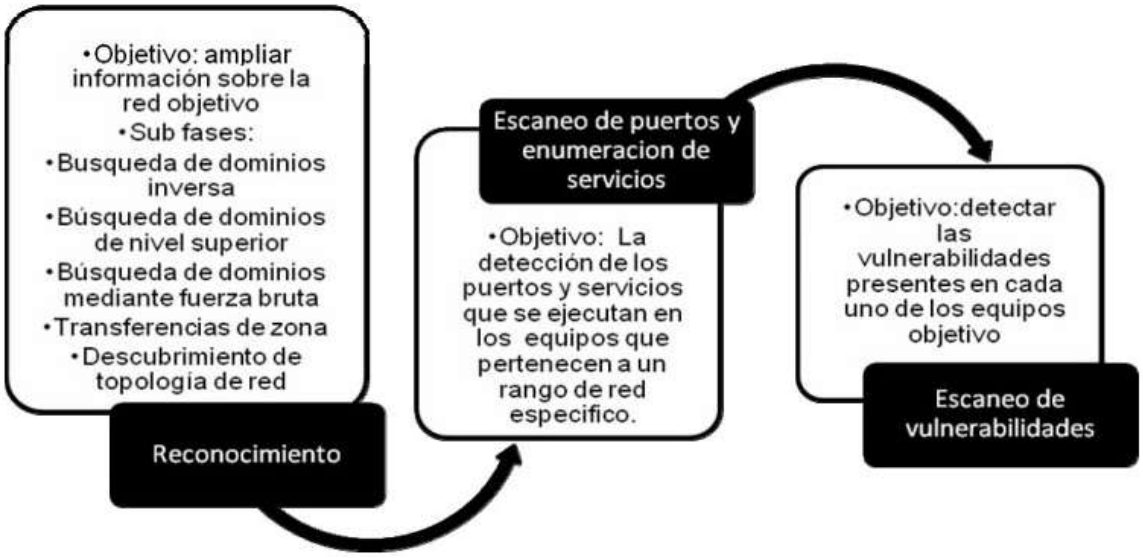
Categoría de Amenaza	Descripción
Negación de Servicio	El atacante impide o limita el uso normal o la gestión de las redes o la red. Dispositivos.
Escuchar a escondidas (Eavesdropping)	El atacante monitorea pasivamente las comunicaciones de red en busca de datos, incluida la autenticación. Cartas credenciales.
Hombre en el medio(Man-in-the-Middle)	El atacante se hace pasar activamente por varias partes legítimas, como aparecer como un cliente para un AP y aparece como un AP para un cliente. Permite al atacante interceptar comunicaciones. Entre un AP y un cliente, obtiene así datos y credenciales de autenticación.
Enmascarado(Masquerading)	El atacante se hace pasar por un usuario autorizado y obtiene ciertos privilegios no autorizados.
Modificación de mensajes (Message Modification)	El atacante altera un mensaje legítimo elimina, agrega, cambia o reordena.
Repetición de mensajes(Message Reply)	El atacante monitorea pasivamente las transmisiones y retransmite mensajes, actúa como si el atacante era un usuario legítimo.
Malversación(Misappropriation)	El atacante roba o hace uso no autorizado de un servicio.
Análisis de tráfico (Traffic Analysis)	El atacante monitorea pasivamente las transmisiones para identificar patrones de comunicación y Participantes.

Fuente: tomado a partir de la IEEE802.11 (2022).

2.3.4. Detectar (*Detect*):

Se detectan los soportes de control y manejo de almacenamiento de datos, se encuentran actividades inusuales de la red. Según el artículo Metodología para la detección de Vulnerabilidades en redes de datos publicado en la revista Cielo (2012), Por lo tanto, es importante cumplir con las tres fases para la detección de vulnerabilidades como lo muestra el gráfico 9.

Gráfico 9: Metodología para la detección de vulnerabilidades.



Fuente: tomado de la Metodología detección de vulnerabilidades David A. (2012)

En cuanto a la aplicación de las fases para detección de vulnerabilidades, se detalla en la aplicación del checklist de NIST categoría Monitoreo continuo del estado actual encontrado.

Anomalías y Eventos (DE.AE): Se detectan de manera oportuna las actividades anómalas ante potenciales eventos de impacto para la organización. Según lo detallado en la NIST 800-94 Rev1 (2012). En la Guía de Sistemas de Detección y Prevención de Intrusiones con sus siglas (IDPS), existe una tabla comparativa de tipos de intrusiones por tecnología como está detallado en la tabla 11.

Tabla 11: Comparativo de IDPS por tipos de tecnología

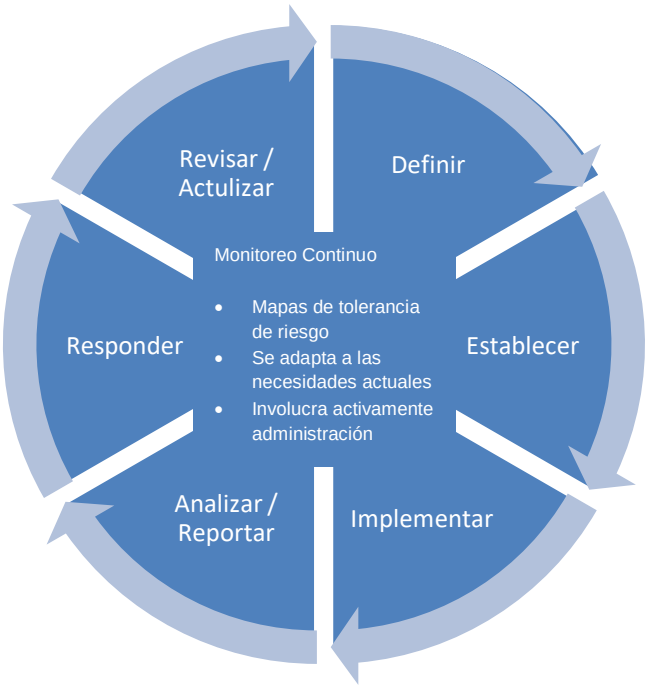
Tipo de tecnología IDPS	Tipos de Actividades Maliciosas detectadas	Alcance por sensor o agente	Fortalezas
Basado en red	Red, transporte y aplicación capa TCP/IP actividad	Red múltiple subredes y grupos de anfitriones	Capaz de analizar la más amplia gama de protocolos de aplicación; solo los IDPS que analizan a fondo muchos de ellos
Inalámbrico	Actividad de protocolo inalámbrico; local inalámbrico no autorizado redes de área (WLAN) en uso	Múltiples WLAN y grupos de clientes inalámbricos	Solo IDPS que permiten monitorear redes inalámbricas actividad de protocolo
Análisis de comportamiento de red (NBA)	Actividad de capa TCP/IP de red, transporte y aplicación que provoca flujos de red anómalos	Red múltiple subredes y grupos de anfitriones	Típicamente más efectivo que los otros en identificación de exploración de reconocimiento y ataques DoS y en la reconstrucción de importantes infecciones de malware
Basado en Host	Aplicación host y funcionamiento actividad del sistema (SO); red, transporte y aplicación Actividad de la capa TCP/IP	Individual host	Solo los IDPS que permiten analizar la actividad que fue transferido en cifrado de extremo a extremo comunicaciones

Fuente: tomado a partir de NIST 800-94rev1 (2012).

Monitoreo Continuo de Seguridad (DE.CM):

Existe un monitoreo por intervalos para identificar eventos en ciberseguridad y verificar la efectividad de medidas de protección existentes. En el gráfico 10, se especifica el proceso de monitoreo continuo de Seguridad de la información.

Gráfico 10: Monitoreo Continuo de seguridad de la Información



Fuente: tomado a partir de NIST 800-137 (2011)

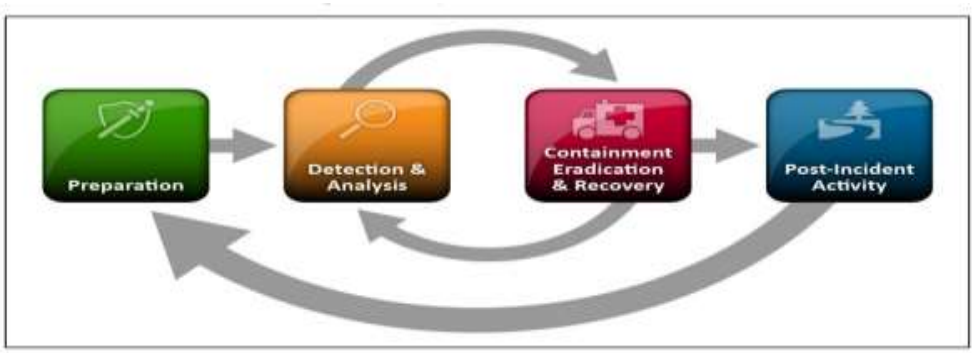
2.3.5. Responder (*Respond*):

Se realiza un plan para mantener en funcionamiento correcto las operaciones del negocio.

Planificación de respuestas (RS.RP): Existen procesos y procedimientos de respuesta, para obtener una respuesta oportuna a los incidentes de ciberseguridad

detectados. Para el correcto manejo de respuesta de incidentes 800-61r2 (2012), se detalla el gráfico 11.

Gráfico 11: Ciclo de Respuesta a incidentes



Fuente: tomado a partir de NIST 800-61r2.

Comunicaciones (RS.CO):

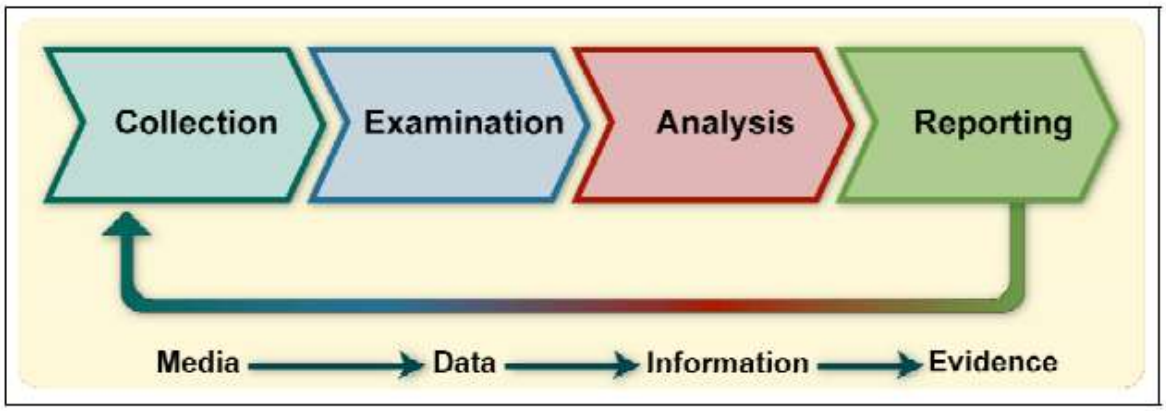
Existe una coordinación de actividades de respuesta con organismos internos y externos para el cumplimiento de la ley en actividades de respuesta si son requeridas.

Según la ISO 27001 16.1.5 (2013), es importante aprender de los incidentes de seguridad de la información, para cumplir con ello es necesario llevar un control, guía de implementación y otra información que permita minimizar la ocurrencia, del daño y el gasto de posibles accidentes de seguridad en las comunicaciones de la organización.

Análisis (RS.AN):

Existe un análisis para garantizar una respuesta adecuada a cada incidente y con ello dar un apoyo en las actividades de recuperación. Para el correcto proceso de análisis la NIST 800-86 (2006) determina cuatro elementos que se toma en el proceso forense como lo determina el gráfico 12. En el mismo se detalla la necesidad de cuatro pasos necesarios para la identificación de datos potenciales y recopilarlos, en primera fase se examinan estos datos lo que implica su evaluación y extracción de información relevante, en la fase dos se analizan los datos para extraer conclusiones, para cumplir con este objetivo el analista forense utiliza un enfoque metódico, en la fase final se realiza un informe para la presentación de la información resultante de la fase de análisis.

Gráfico 12: Proceso Forense



Fuente: tomado a partir de NIST 800-86 (2006).

Mitigación (RS.MI):

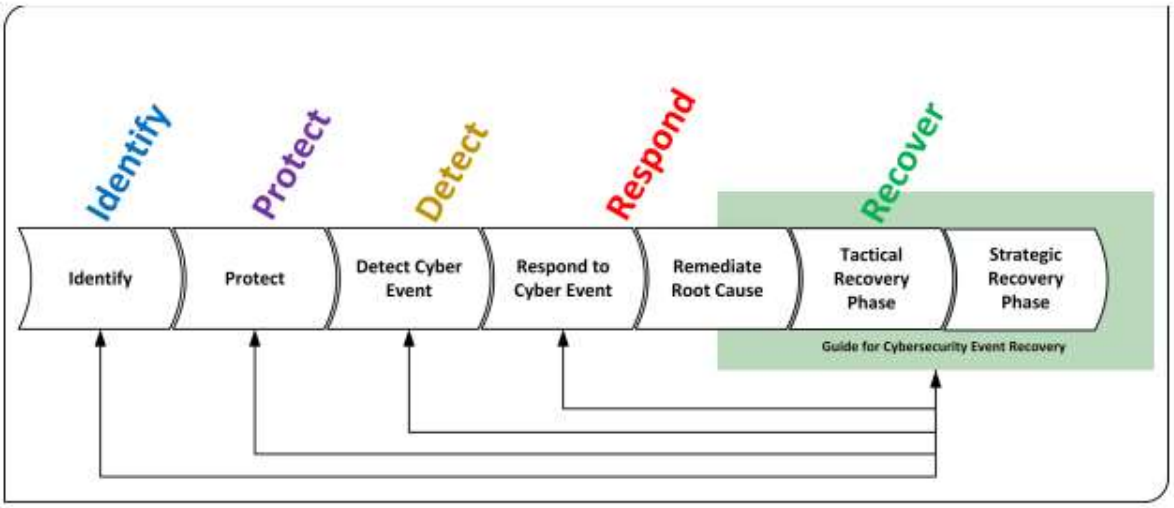
Con las actividades realizadas, se previene la expansión de eventos, mitigar sus efectos y con ello resolver los incidentes presentados. El marco de trabajo de NIST 800-83r1 (2013), determina que es importante realizar la prevención de incidentes posibles en la organización y con ello determinar las respuestas necesarias para mitigar sus efectos críticos de impacto.

2.3.5. Recuperar (*Recover*):

Permite reparar y restaurar los equipos y red luego de una afectación.

Planificación de la Recuperación (RC.RP): Se ejecutan procesos y procedimientos de recuperación para garantizar la restauración oportuna de activos y sistemas afectados por incidentes de ciberseguridad presentados. Dentro del marco de trabajo de NIST indica que cada componente del marco de trabajo necesita retroalimentación para identificar mejoras a partir de lecciones aprendidas por eventos cibernéticos, con estas lecciones se impulsan las mejoras para una correcta planificación en relación a operaciones de seguridad, políticas, etc. En el gráfico 13, se evidencia la relación de cada uno de los componentes del marco de trabajo de NIST.

Gráfico 13: Guía para la recuperación de eventos de ciberseguridad relacionados NIST



Fuente: tomado a partir de NIST 800-184 (2016).

2.4. Fases de implementación de NIST

Para la correcta implementación del marco de trabajo, se requiere de 7 fases como hoja de ruta las mismas que se las detallar a continuación: Priorización y Alcance: Se identifican los objetivos de la organización, para la correcta implementación de ciberseguridad en la institución.

Orientación: Se orienta a la organización con la identificación previa realizada en cuanto a sus activos. Perfil Actual: Se lanza la hoja de ruta de NIST en busca de resultados en cada una de las categorías del marco de trabajo para obtener el perfil actual.

Evaluación de Riesgos: Se evalúa el entorno de la organización para el análisis de riesgos emergentes para mitigar su impacto dentro de ella. Perfil Deseado: Con la hoja de ruta inicial, es necesario verificar los resultados con el perfil objetivo para obtener las brechas encontradas en cada una de las funciones del marco de trabajo de NIST.

Determinar, analizar y priorizar brechas: Con las dos hojas de ruta obtenidas, se crean los perfiles en cada una de las funciones del marco de trabajo para priorizar las brechas encontradas. Implementar plan de Acción:

En el plan de acción, se determinan cada una de las acciones a tomar para minimizar los riesgos.

CAPÍTULO III: ANÁLISIS DE RESULTADOS

3.1. Proceso de implementación de NIST

Para la implementación del marco de trabajo de NIST, se cumplen 7 pasos que se describen a continuación.

3.1.1 Priorizar el alcance

En este paso del marco de trabajo NIST, se detallan las necesidades organizacionales y decisiones estratégicas con respecto a la implementación de ciberseguridad. En la tabla 12 se detalla la información general de la institución.

Tabla 12: Priorización alcance

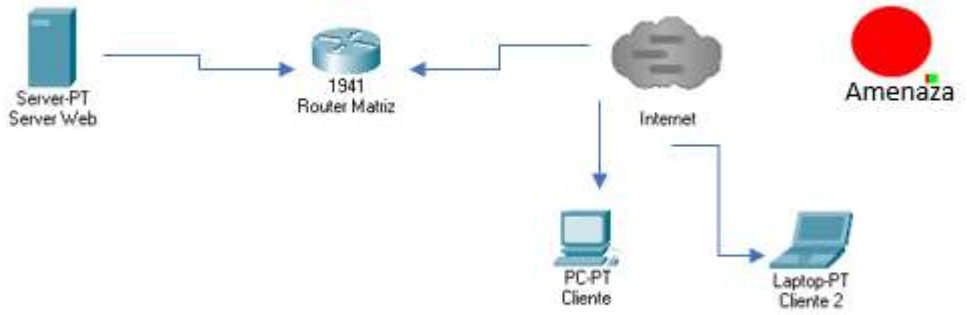
Información General	
Nombre	Instituto Superior Tecnológico Sucre
Sector	Educativo
Objetivo de negocio	Brindar servicios educativos
Misión	N/A
Visión	N/A
Cantidad de procesos	6
# empleados	166
Portales Web	Sistema de notas Sistema de evaluación Docente Sitio web

Fuente: elaboración propia con información del ITS SUCRE.

3.1.2. Orientar

Al ser una institución educativa el alcance de su programa de ciberseguridad está orientada en la protección de sus equipos, datos e infraestructura crítica encontrada en el análisis de priorización. En el gráfico 14, se determina la infraestructura encontrada en la organización.

Gráfico 14: Estructura Servidor Web

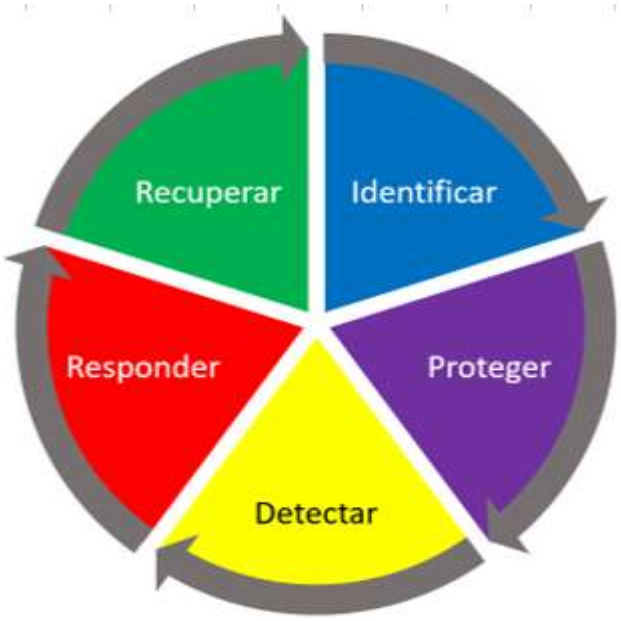


Fuente: elaboración propia a partir de la estructura Servidor web ITS SUCRE

3.1.3. Crear un perfil Actual

Para obtener el perfil actual se lanzó una encuesta del marco de trabajo NIST, al área de TIC de la IES. En el gráfico 7, se evidencian las funciones del marco de trabajo de NIST. En el gráfico 15, se detallan los perfiles del marco de trabajo de NIST.

Gráfico 15: Elementos del marco de trabajo



Fuente: tomado de NIST (2018)

Cada una de las funciones del marco de trabajo están detalladas por categorías como lo detalla el gráfico 16.

Gráfico 16: Categorías del Marco de trabajo de NIST.

Identificador único de función	Función	Identificador único de categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
		ID.BE	Entorno empresarial
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	Proteger	PR.AC	Gestión de identidad y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología protectora
DE	Detectar	DE.AE	Anomalías y eventos
		DE.CM	Vigilancia continua de seguridad
		DE.DP	Procesos de detección
RS	Responder	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
RC	Recuperar	RC.RP	Planificación de recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Fuente: tomado de las categorías del Marco de trabajo NIST (2018)

Cada categoría tiene una subcategoría como está detallado en el gráfico 16. Subcategorías del marco de trabajo NIST.

Para la creación del perfil actual en la institución, se inicia de niveles de implementación detallados en por marco de trabajo NIST como lo determina el gráfico 17.

Gráfico 17: Niveles de implementación NIST

Fuente: tomado de NIST (2018)

Para realizar el cálculo del estado actual, se utiliza la siguiente valoración determinada por el marco de trabajo de NIST, como lo determina la tabla 13.

Nivel: El marco de trabajo de NIST, se implementa en cuatro niveles como está detallado en el gráfico 17.

Logro: Están determinados por cada uno de los niveles alcanzados como Parcial, Riesgo Informado, Repetible, Adaptado.

Descripción: Determina si existe hasta la correcta aplicación del mismo.

Valor: la valoración va desde un 25% hasta 100%, según el nivel alcanzado.

Tabla 13: Determinación de porcentaje de logro

Nivel	Logro	Descripción	Valor
1	Parcial	Logro no existe o no fue reportado	25%
2	Riesgo Informado	Logro fue reportado	50%
3	Repetible	Logro se encuentra determinado, pero no tiene una política	75%
4	Adaptable	Logro se encuentra aplicado dentro de las políticas	100%

Fuente: tomado de NIST (2018)

A continuación, se detallan los porcentajes obtenidos por categorías evaluadas para determinar el perfil actual en la tabla 14. Para llegar a estos resultados se toma en cuenta los porcentajes de logro de la tabla 13.

Función: Se detalla cada una de las categorías del marco de trabajo de NIST

Categoría: Es el código de acuerdo al checkList de NIST, ver gráfico 17

%Logro: Se determina el porcentaje obtenido de acuerdo a la tabla 13, sumado y dividido por el máximo logro obtenido

Ejemplo: Función identificar 6 logros nivel 1+ 1+ 1+ 1+ 1+ 1 =6/24 = 0,25=25%

Máximo de logro que se obtiene 4+4+4+4+4+4=24/24=1 =100%, ver tabla 13.

Tabla 14: Logros alcanzados en la primera aplicación del Checklist de NIST

Función	Categoría	%Logro
IDENTIFICAR(ID)	ID.AM	25%
	ID.BE	30%
	ID.GV	25%
	ID.RA	29,17%
	ID.RM	25%
	ID.SC	30%
FUNCIÓN ID		27,36%
PROTEGER(PR)	PR.AC	35,71%
	PR.AT	30%
	PR.DS	31,25%
	PR.IP	35,42%
	PR.MA	37,50%
	PR.PT	40%
FUNCIÓN PR		34,98%
DETECTAR(DE)	DE.AE	40%
	DE.CM	25%
	DE.DP	30%
FUNCIÓN DE		31,67%
RESPONDER(RS)	RS.RP	25%
	RS.CO	35%
	RS.AN	30%
	RS.MI	33,33%
	RS.IM	25%
FUNCIÓN RS		29,67%
RECUPERAR(RC)	RC.RP	25%
	RC.IM	25%
	RC.CO	33%
FUNCIÓN RC		27,78%

Fuente: elaboración propia aplicación Marco de trabajo NIST.

3.1.4. Realizar una evaluación de riesgos

En NIST 800-60, determina que un activo está determinado por Disponibilidad, Integridad y Confidencialidad, es decir toma tres niveles de impacto para un activo.
Confidencialidad: La información es accesible sólo por personal autorizado.
Integridad: Los datos están como el emisor la genero, no se manipula por terceros.
Disponibilidad: La información está disponible siempre para el personal autorizado.
Con las definiciones anteriores, se determina la tabla 15 para la valoración de impacto de un activo según NIST.

Tipo: Según la ISO 27001, la valoración de activos se la realiza como lo detalla la tabla 15. Criticidad: Se basa en confidencialidad, integridad y disponibilidad de los activos, para ser alta cumple con al menos dos de ellos, para ser media tiene que cumplir al menos uno de ellos, baja si no presenta ninguna de estas criticidades.

Tabla 15: Valores de la información de un activo

Tipo	Criticidad
ALTA	Activos de la información en la cual ,(2) o todas sus propiedades (confidencialidad, integridad, disponibilidad) es alta
MEDIA	Activos de información donde la clasificación de la información es alta en una (1) de sus propiedades y al menos una de ellas es medio
BAJA	Activos de información en los cuales todos sus niveles son bajos

Fuente: tomado de la ISO 27001 (2005)

Con la aplicación de la tabla 15, determina la criticidad de cada uno de los activos para valorarlos y saber cuáles están protegidos de forma urgente. En la tabla 16, se detallan los activos según su criticidad para su revisión de brecha para el plan de acción institucional.

ID: Está determinado por los códigos asignados por el departamento de TICS
Activo: Se define el nombre físico del activo asignado al activo

Tipo de Activo: Se determina a donde pertenece el activo

Criticidad: Es el cálculo asignado al activo a través de la valoración de activos de la tabla 15.

Tabla 16: Valoración de activos

ID	Activo	Tipo de Activo	Criticidad			
			Confidencialidad	Integridad	Disponibilidad	Medio Criticidad
1	Servidor	Organizacional	3-Alto	3-Alto	3-Alto	3,00
2	Router	Organizacional	3-Alto	3-Alto	3-Alto	3,00
3	Switch	Organizacional	3-Alto	3-Alto	3-Alto	3,00
4	Red datos	Organizacional	2-Medio	2-Medio	2-Medio	2,00
5	Red Inalámbrica	Organizacional	1-Bajo	1-Bajo	1-Bajo	1,00
6						

Fuente: elaboración propia a partir de los activos ITS SUCRE

Con los resultados obtenidos de la identificación de amenazas, se determina la clasificación del nivel de riesgo en cada uno de los activos para determinar su perfil actual. En la tabla 17 detalla la identificación de amenazas encontradas.

Activo: Nombre del activo encontrado Tipo Activo: Determinación de activos a partir de los activos del ITS SUCRE. Amenaza: Determinación si pertenece a hardware o software. Probabilidad: Probabilidades según las amenazas encontradas para el activo. Impacto: Qué impacto tiene la organización por la amenaza encontrada. Nivel de Riesgo: Clasifica el activo de acuerdo con la tabla de riesgos.

Tabla 17: Identificación de amenazas

Activo	Tipo de Activo	Amenaza	Probabilidad	Impacto	Nivel de Riesgo
Servidor WEB	HARDWARE	No se realizan los cambios de clave periódicamente PR.AC-1	Filtración de clave ocasiona accesos no permitidos	Robo de información	3-Alto
Centro de Datos	HARDWARE	No cuenta con seguridad perimétrica PR.AC-2	Al no tener acceso por privilegios permite el acceso por personal no autorizado	Daño de equipo o robo de los mismos	3-Alto
Integridad de la Red de Datos	HARDWARE	No existe segmentación de redes de datos PR.AC-5	La red cableada no maneja una estructura segmentada para evitar bloqueos de accesos no deseados	Accesos no deseados a la información	3-Alto

Fuente: tomado a partir de identificación de amenazas de NIST.

3.1.5 Crear un perfil de destino

El perfil de destino está dado con la comparativa que se realizó frente al perfil actual para obtener el cumplimiento si fue cumplido en el tiempo establecido el detalle obtenido en el checklist está detallado en la tabla 18.

Función: Se detalla cada una de las categorías del marco de trabajo de NIST. Categoría: Es el código de acuerdo al checkList de NIST, ver gráfico 17 %Logro: Se determina el porcentaje obtenido de acuerdo a la tabla 13, sumado y dividido por el máximo logro obtenido. Ejemplo: Función identificar 6 logros nivel 3+4+4+2+2+4 =19/24 = 0,7917=79,17%. Máximo de logro que se obtiene 4+4+4+4+4+4=24/24=1 =100%, ver tabla 13.

Tabla 18: Perfil Objetivo

Función	Categoría	%Logro
IDENTIFICAR(ID)	ID.AM	79,17%
	ID.BE	65%
	ID.GV	56,25%
	ID.RA	79,17%
	ID.RM	58,33%
	ID.SC	60%
FUNCIÓN ID		66,32%
PROTEGER(PR)	PR.AC	78,57%
	PR.AT	80%
	PR.DS	68,75%
	PR.IP	64,58%
	PR.MA	62,50%
	PR.PT	70%
FUNCIÓN PR		70,73%
DETECTAR(DE)	DE.AE	65%
	DE.CM	62,50%
	DE.DP	50%
FUNCIÓN DE		59,17%
RESPONDER(RS)	RS.RP	50%
	RS.CO	50%
	RS.AN	60%
	RS.MI	50%

	RS.IM	50%
FUNCIÓN RS		52%
RECUPERAR(RC)	RC.RP	50%
	RC.IM	62,50%
	RC.CO	50%
FUNCIÓN RC		54,17%

Fuente: elaboración propia Checklist NIST

3.1.6 Determinar, analizar y priorizar brechas

Con la ayuda de los checklist realizados y los perfil actual y objetivo determinado a un periodo de 6 meses se obtuvieron las brechas que determinan las prioridades que van a ser definidas dentro del plan de acción institucional. Los análisis de resultados están detallados en la tabla 19.

Función: Identificar (ID), es la primera del núcleo de NIST y tiene 6 categorías y estas a su vez manejan sus propias subcategorías como lo detalla la tabla 19.
Gestión de Activos (ID.AM): Evalúa los datos, el personal, los dispositivos, los sistemas y las instalaciones para cumplir con los propósitos comerciales de la organización.

Entorno Empresarial (ID.BE): En base a la misión y objetivos se determinan los roles de ciberseguridad para delegar responsabilidades dentro de la organización. Gobernanza (ID. GV): Se regulan legalmente los procesos para una correcta gestión de riesgos en ciberseguridad. Evaluación de Riesgos (ID.RA): Se verifica si la organización comprende los riesgos en ciberseguridad en sus operaciones institucionales.

Estrategia de gestión de Riesgos (ID.RM): Evalúa si existen prioridades en los riesgos institucionales. Gestión de Riesgos de la Cadena de Suministro (ID.SC): Realiza la evaluación si los proveedores externos manejan una correcta evaluación de riesgos.

Tabla 19: Subcategorías Identificar

IDENTIFICAR						
Gestión de Activos (ID.AM)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
ID.AM-1	Parcial	1	Repetible	3	2	Media
ID.AM-2	Parcial	1	Adaptable	4	3	Alta
ID.AM-3	Parcial	1	Adaptable	4	3	Alta
ID.AM-4	Parcial	1	Riesgo Informado	2	1	Baja
ID.AM-5	Parcial	1	Riesgo Informado	2	1	Baja
ID.AM-6	Parcial	1	Adaptable	4	1	Alta
IDENTIFICAR						
Entorno Empresarial (ID.BE)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
ID.BE-1	Parcial	1	Riesgo Informado	2	1	Baja
ID.BE-2	Parcial	1	Riesgo Informado	2	1	Baja
ID.BE-3	Parcial	1	Riesgo Informado	2	1	Baja
ID.BE-4	Parcial	1	Adaptable	4	3	Alta
ID.BE-5	Riesgo Informado	2	Repetible	3	1	Baja

IDENTIFICAR						
Gobernanza (ID.GV)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
ID.GV-1	Parcial	1	Riesgo Informado	2	1	Baja
ID.GV-2	Parcial	1	Repetible	3	2	Media
ID.GV-3	Parcial	1	Riesgo Informado	2	1	Baja
ID.GV-4	Parcial	1	Riesgo Informado	2	1	Baja
DENTIFICAR						
Evaluación de Riesgos (ID.RA)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
ID.RA-1	Parcial	1	Riesgo Informado	3	2	Media
ID.RA-2	Riesgo Informado	2	Repetible	4	2	Media
ID.RA-3	Parcial	1	Riesgo Informado	4	3	Alta
ID.RA-4	Parcial	1	Riesgo Informado	2	1	Baja
ID.RA-5	Parcial	1	Riesgo Informado	4	3	Alta
ID.RA-6	Parcial	1	Riesgo Informado	2	1	Baja
IDENTIFICAR						
Estrategia de Gestión de Riesgos (ID.RM)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
ID.RM-1	Parcial	1	Riesgo Informado	2	1	Baja
ID.RM-2	Parcial	1	Riesgo Informado	2	1	Baja
ID.RM-3	Parcial	1	Repetible	3	2	Media
IDENTIFICAR						
Gestión del riesgo de la cadena de suministro (ID.SC)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
ID.SC-1	Riesgo Informado	2	Adaptable	4	2	Media
ID.SC-2	Parcial	1	Riesgo Informado	2	1	Baja
ID.SC-3	Parcial	1	Riesgo Informado	2	1	Baja
ID.SC-4	Parcial	1	Riesgo Informado	2	1	Baja

Función: Proteger (PR), es la segunda del núcleo de NIST y tiene 6 categorías y estas a su vez manejan sus propias subcategorías como lo detalla la tabla 20. Gestión de Identidades, Autenticación y Control de Acceso (PR.AC): Permite obtener la gestión de accesos y permisos a los dispositivos utilizados por los usuarios. Concienciación y Capacitación (PR.AT): Evalúa los roles y las capacitaciones a los usuarios de los sistemas organizacionales.

Seguridad de Datos (PR.DS): Se obtiene información de la gestión de activos en relación al manejo de datos. Procesos y Procedimientos de Protección de la Información (PR. IP): Se evalúa la correcta elaboración de procesos de respaldos de seguridad en la organización. Mantenimiento (PR.MA): Se verifica si existen herramientas aprobadas para el correcto mantenimiento de los activos organizacionales. Tecnología de Protección (PR.PT): Se evalúa si existen auditorías de la documentación de activos y si existe una revisión periódica de su correcto manejo.

Tabla 20: Brechas Proteger

PROTEGER						
Gestión de identidad, autenticación y control de acceso (PR.AC)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
PR.AC-1	Parcial	1	Riesgo Informado	2	1	Baja
PR.AC-2	Parcial	1	Adaptable	4	3	Alta
PR.AC-3	Riesgo Informado	2	Adaptable	4	2	Media
PR.AC-4	Riesgo Informado	2	Adaptable	4	2	Media
PR.AC-5	Parcial	1	Riesgo Informado	2	1	Baja
PR.AC-6	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo cumplido
PR.AC-7	Parcial	1	Riesgo Informado	2	1	Baja

PROTEGER						
Concienciación y capacitación (PR.AT)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
PR.AT-1	Parcial	1	Adaptable	4	3	Alta
PR.AT-2	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo Alcanzado
PR.AT-3	Parcial	1	Riesgo Informado	2	1	Baja
PR.AT-4	Parcial	1	Adaptable	4	3	Alta
PR.AT-5	Parcial	1	Adaptable	4	3	Alta
ROTEGER						
Seguridad de los datos (PR.DS)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
PR.DS-1	Parcial	1	Adaptable	4	3	Alta
PR.DS-2	Parcial	1	Adaptable	4	3	Alta
PR.DS-3	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo Alcanzado
PR.DS-4	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo Alcanzado
PR.DS-5	Parcial	1	Riesgo Informado	2	1	Baja
PR.DS-6	Parcial	1	Riesgo Informado	2	1	Objetivo Alcanzado
PR.DS-7	Parcial	1	Adaptable	4	3	Alta
PR.DS-8	Parcial	1	Riesgo Informado	2	1	Baja
PROTEGER						
Procesos y procedimientos de protección de la Información (PR.IP)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
PR.IP-1	Parcial	2	Riesgo Informado	2	0	Objetivo Alcanzado
PR.IP-2	Parcial	1	Riesgo Informado	2	1	Baja
PR.IP-3	Riesgo Informado	1	Adaptable	4	3	Alta
PR.IP-4	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo Alcanzado
PR.IP-5	Parcial	2	Riesgo Informado	2	0	Objetivo Alcanzado
PR.IP-6	Riesgo Informado	1	Riesgo Informado	2	1	Baja
PR.IP-7	Parcial	2	Adaptable	4	2	Media
PR.IP-8	Parcial	2	Riesgo	2	0	Objetivo

			Informado			Alcanzado
PR.IP-9	Parcial	1	Adaptable	4	3	Alta
PR.IP-10	Parcial	1	Repetible	3	2	Media
PR.IP-11	Parcial	1	Riesgo Informado	2	1	Baja
PR-IP-12	Parcial	1	Riesgo Informado	2	1	Baja
PROTEGER						
Procesos y procedimientos de protección de la información (PR.MA)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
PR.MA-1	Parcial	1	Repetible	3	2	Media
PR.MA-2	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo Alcanzado
PROTEGER						
Tecnología de protección (PR.PT)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
PR.PT-1	Parcial	1	Adaptable	4	3	Alta
PR.PT-2	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo Alcanzado
PR.PT-3	Riesgo Informado	2	Repetible	3	1	Baja
PR.PT-4	Riesgo Informado	2	Repetible	3	1	Baja
PR.PT-5	Parcial	1	Riesgo Informado	2	1	Baja

Fuente: elaboración propia del Checklist NIST.

Función: Detectar (DE), es la tercera del núcleo de NIST y tiene 3 categorías y estas a su vez manejan sus propias subcategorías como lo detalla la tabla 21. Anomalías y Eventos (DE.AE): Se evalúan si se gestionan los eventos detectados y su información es recopilada correctamente. Monitoreo Continuo de la Seguridad (DE.CM): Evalúa si existen un monitoreo constante de eventos y si existe personal asignado para su evaluación. Procesos de Detección (DE.DP): En la evaluación, se determina la existencia de roles y si se prueban los procesos de detección.

Tabla 21: Brechas Detectar

DETECTAR						
Anomalías y Eventos (DE.AE)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
DE.AE-1	Parcial	1	Repetible	2	1	Baja
DE.AE-2	Riesgo Informado	2	Repetible	2	0	Objetivo Alcanzado
DE.AE-3	Parcial	1	Repetible	4	3	Alta
DE.AE-4	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo Alcanzado
DE.AE-5	Riesgo Informado	2	Riesgo Informado	3	1	Baja
DETECTAR						
Monitoreo Continuo de la seguridad (DE.CM)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
DE.CM-1	Parcial	1	Repetible	3	2	Media
DE.CM-2	Parcial	1	Repetible	3	2	Media
DE.CM-3	Parcial	1	Repetible	3	2	Media
DE.CM-4	Parcial	1	Riesgo Informado	2	1	Baja
DE.CM-5	Parcial	1	Riesgo Informado	2	1	Baja
DE.CM-6	Parcial	1	Riesgo Informado	2	1	Baja
DE.CM-7	Parcial	1	Riesgo Informado	2	1	Baja
DE.CM-8	Parcial	1	Repetible	3	2	Media
ETECTAR						
Procesos de Detección (DE.DP)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
DE.DP-1	Parcial	1	Riesgo Informado	2	1	Baja
DE.DP-2	Parcial	1	Riesgo Informado	2	1	Baja
DE.DP-3	Parcial	1	Riesgo Informado	2	1	Baja
DE.DP-4	Riesgo Informado	2	Riesgo Informado	2	1	Objetivo Alcanzado
DE.DP-5	Parcial	1	Riesgo Informado	2	1	Baja

Fuente: elaboración propia del Checklist NIST.

Función: Responder (RS), es la tercera del núcleo de NIST y tiene 5 categorías y estas a su vez manejan sus propias subcategorías como lo detalla la tabla 22. Planificación de la Respuesta(RS.RP):Evalúa la existencia de un plan de respuesta a incidentes cibernéticos. Comunicaciones (RS.CO): Esta categoría evalúa las actividades de respuesta existentes en la organización.

Análisis (RS.AN): Se evalúa la existencia de investigaciones de las notificaciones de eventos cibernéticos y sus respectivos análisis. Mitigación (RS.MI): En la evaluación, se determina la existencia de respuesta a incidentes contenidos y mitigados. Mejoras (RS.IM): Evalúa las actividades de respuesta de la organización incorpora planes de respuesta como lecciones para mejoramiento continuo.

Tabla 22: Brechas Responder

RESPONDER						
Planificación de la respuesta (RS.RP)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
RS.RP-1	Parcial	1	Riesgo Informado	2	1	Baja
RESPONDER						
Comunicaciones (RS.CO)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
RS.CO-1	Parcial	1	Riesgo Informado	2	1	Baja
RS.CO-2	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo Alcanzado
RS.CO-3	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo Alcanzado
RS.CO-4	Parcial	1	Riesgo Informado	2	1	Objetivo Alcanzado
RS.CO-5	Parcial	1	Riesgo Informado	2	1	Baja
RESPONDER						
Análisis (RS.AN)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad

RS.AN-1	Parcial	1	Repetible	3	2	Media
RS.AN-2	Parcial	1	Riesgo Informado	2	1	Baja
RS.AN-3	Parcial	1	Riesgo Informado	2	1	Baja
RS.AN-4	Parcial	1	Riesgo Informado	2	1	Baja
RS.AN-5	Riesgo Informado	2	Repetible	3	1	Baja
RESPONDER						
Mitigación (RS.MI)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
RS.MI-1	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo Alcanzado
RS.MI-2	Parcial	1	Riesgo Informado	2	1	Baja
RS.MI-3	Parcial	1	Riesgo Informado	2	1	Baja
RESPONDER						
Mejoras (RS.IM)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
RS.IM-1	Parcial	1	Riesgo Informado	2	1	Baja
RS.IM-2	Parcial	1	Riesgo Informado	2	1	Baja

Fuente: elaboración propia del Checklist NIST.

Función: Recuperar (RC), es la tercera del núcleo de NIST y tiene 3 categorías y estas a su vez manejan sus propias subcategorías como lo detalla la tabla 23. Planificación de la Recuperación (RC.RP):Evalúa la existencia de una plan institucional en recuperación de incidentes de seguridad cibernética. Mejoras (RC.IM): Esta Subcategoría evalúa si los planes de recuperación manejas lecciones aprendidas.Comunicaciones (RC.CO): Determina si las actividades de recuperación son comunicadas a las partes interesadas de la organización.

Tabla 23: Brechas Recuperar

RECUPERAR						
Planificación de la recuperación (RC.RP)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
RC.RP-1	Parcial	1	Riesgo Informado	2	1	Baja
RECUPERAR						
Mejoras (RC.IM)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
RC.IM-1	Parcial	1	Repetible	3	1	Media
RC.IM-2	Parcial	1	Riesgo Informado	2	1	Baja
RECUPERAR						
Comunicaciones (RS.CO)						
	Estado Actual		Objetivo Deseado		Prioridad	
SUBCATEGORÍA	Logro	Nivel	Logro	Nivel	Brecha	Prioridad
RC.CO-1	Parcial	1	Riesgo Informado	2	1	Baja
RC.CO-2	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo Alcanzado
RC.CO-3	Parcial	1	Riesgo Informado	2	1	Baja

Fuente: elaboración propia del Checklist NIST.

Función: Detalle de cada una de las funciones del marco de trabajo de NIST.

Categoría: Desglose de cara una de las categorías por cada función del marco de trabajo de NIST.%Logro Actual: Detalla el porcentaje alcanzado según el estado actual institucional.%Logro Deseado: Luego de las metas propuestas, se detalla el alcance en cada una de las funciones del marco de trabajo de NIST.%Brecha: Con los perfiles actual y deseado, se obtiene las brechas existentes para cada categoría del marco.

Tabla 24: Resultados Perfil actual Vs Perfil Objetivo

Función	Categoría	%Logro Actual	%Logro Deseado	%Brecha
IDENTIFICAR(ID)	ID.AM	25%	79,17%	54,17%
	ID.BE	30%	65%	35%
	ID.GV	25%	56,25%	31,25%
	ID.RA	29,17%	79,17%	50%
	ID.RM	25%	58,33%	33,33%
	ID.SC	30%	60%	30%
FUNCIÓN ID		27,36%	66,32%	38,96%
PROTEGER(PR)	PR.AC	35,71%	78,57%	42,86%
	PR.AT	30%	80%	50%
	PR.DS	31,25%	68,75%	37,50%
	PR.IP	35,42%	64,58%	29,17%
	PR.MA	37,50%	62,50%	25%
	PR.PT	40%	70%	30%
FUNCIÓN PR		34,98%	70,73%	35,75%
DETECTAR(DE)	DE.AE	40%	65%	25%
	DE.CM	25%	62,50%	37,50%
	DE.DP	30%	50%	20%
FUNCIÓN DE		31,67%	59,17%	27,50%
RESPONDER(RS)	RS.RP	25%	50%	25%
	RS.CO	35%	50%	15%
	RS.AN	30%	60%	30%
	RS.MI	33,33%	50%	16,67%
	RS.IM	25%	50%	25%
FUNCIÓN RS		29,67%	52%	22,33%
RECUPERAR(RC)	RC.RP	25%	50%	25%
	RC.IM	25%	62,50%	37,50%
	RC.CO	33%	50%	16,67%
FUNCIÓN RC		27,78%	54,17%	26,39%

Fuente: elaboración propia del CheckList NIST.

3.1.7 Implementar un plan de acción

	INSTITUTO SUPERIOR TECNOLÓGICO “SUCRE” PLANIFICACIÓN ESTRATÉGICA 2021-2025 PLAN DE ACCIÓN

Objetivo estratégico	Incrementar estándares de calidad
Estrategia	Estructurar políticas en ciberseguridad para asegurar los sistemas institucionales, base de datos e infraestructura institucional
Tipo de plan	Plan de mejora
Nombre del plan	Plan de mejoramiento continuo en base a las brechas encontradas en la implementación del marco de trabajo de NIST.
Objetivo del plan	Con la implementación de los mejores estándares internacionales en ciberseguridad permitir a la IES ,fortalecer sus controles para alcanzar su etapa de madurez a partir de las brechas según su estado de criticidad
Insumo que sustenta la elaboración del plan	Marco de trabajo de NIST
Indicador de medición del plan de acción	
Meta del plan de acción	
Líder del plan de acción	Ing. Danilo Miniguano Mgs.
Unidad académica o administrativa	Tecnologías de la Información y Comunicación

N.-	ACTIVIDAD	Responsable de la ejecución	Fecha Inicio DD/MM/AA	Fecha Fin DD/MM/AA	Producto/resultado	Evidencia	Presupuesto	Observaciones
1	Inventario Plataformas de	Danilo Miniguan	01/10/2021	01/02/2022	En ejecució	ID.AM-2	1200	Es necesario un inventario inicial de plataformas de software existentes para generar políticas de

	software	o			n			uso. En los inventarios no existe evidencia de plataformas de software pertenecientes a la organización, evidencia tabla 9.
2	Flujos de datos mapeados	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	ID.AM-3	1000	No existe un diagrama del flujo de datos existentes, pese a existir infraestructura de red no se encontró una política de documentación de servicios de red, evidencia tabla 9.
3	Establecimiento de roles y responsabilidades en seguridad cibernética	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	ID.AM-6	1200	No existe un organigrama en TICS define los roles y responsables en ciberseguridad. Solo existe un rol de administración de TICS, más no roles de gestión de riesgos dentro de la organización. Evidencia tabla 8 reglamento institucional.
4	Establecer dependencias de servicios críticos	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	ID.BE-4	1100	Los servicios críticos no se encuentran determinados, es necesario crear un plan de contingencia según las brechas encontradas.
5	Documentación de amenazas internas y externas	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	ID.RA-3	600	No se encontraron documentaciones de reportes de amenazas internas y externas por que se reportó las incidencias para ser tomadas como vulnerabilidades existentes.
6	Determinar riesgos a partir de vulnerabilidades y amenazas existentes	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	ID.RA-5	700	La principal vulnerabilidad reportada está dada por los certificados digitales que no están debidamente utilizados por los aplicativos institucionales. Evidencia tabla 8 de reglamento interno institucional.
7	Protección a los activos físicos	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	PR.AC-2	1200	Los activos físicos como servidores no cuentan con un área adecuado para el correcto funcionamiento dentro de la institución
8	Segmentación de la red física	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	PR.AC-5	1200	La red física institucional no cuenta con una correcta segmentación como lo determinas las normas de NIST y otros estándares especializados
9	Comprensión de roles de los ejecutivos y responsabilidades	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	PR.AT-4	600	No existen roles establecidos que determinen la correcta jerarquía determinada para asegurar las responsabilidades de cada departamento.

10	Comprensión de roles y responsabilidades del personal de seguridad física	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	PR.AT-5	500	No existe personal asignado a la seguridad física y cibernética de la institución
11	Protección de datos	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	PR.DS-1, PR.DS-2	1000	No existen políticas de protección de datos establecidas en la organización
12	Definición de entornos de desarrollo	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	PR.DS-7	600	No existen un entorno de pruebas para complementar el entorno de producción establecido en la organización
13	Establecer procesos de cambios de configuración	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	PR.IP-3	700	No existe una normativa de procesos de control de cambio utilizados actualmente por la organización
14	Plan de respuesta a incidentes y continuidad de negocio	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	PR.IP-10	800	Se notificaron los incidentes encontrados para ser tomados como vitales para la correcta continuidad del negocio como son la disponibilidad de los sistemas académicos y aulas virtuales
15	Política para auditoria de archivos y su documentación	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	PR.PT-1	700	Se determinó el proceso correcto para la creación de una política para la auditoria de activos institucionales
16	Recopilación de datos de eventos encontrados como vulnerables	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	DE.AE-3	600	Se recopiló la información de todas las vulnerabilidades en los sistemas académico y de aulas virtuales que son vitales para el correcto funcionamiento del negocio
17	Plan de recuperación a eventos	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	RC.IM-1	700	En base a las vulnerabilidades encontradas se determina la recuperación de los eventos en el menor tiempo posible para evitar pérdidas económicas para la organización
18	Escaneo de vulnerabilidades periódicas	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	DE.CM-8	600	Se determinó un plan para el escaneo de vulnerabilidades periódicas para encontrar vulnerabilidades a tiempo ,tener una respuesta

								adecuada.
19	Monitoreo de la red periódicamente para detección de posibles eventos de seguridad cibernética	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	DE.CM-3	500	Para el monitoreo periódico de la red se implementaron herramientas de escaneo de red como nmap.
20	Mantenimiento y reparación de activos	Danilo Miniguano	01/10/2021	01/02/2022	En ejecución	PR.MA-1	1000	Con la valoración realizada a los activos de la organización se creó un plan de reparación de activos.

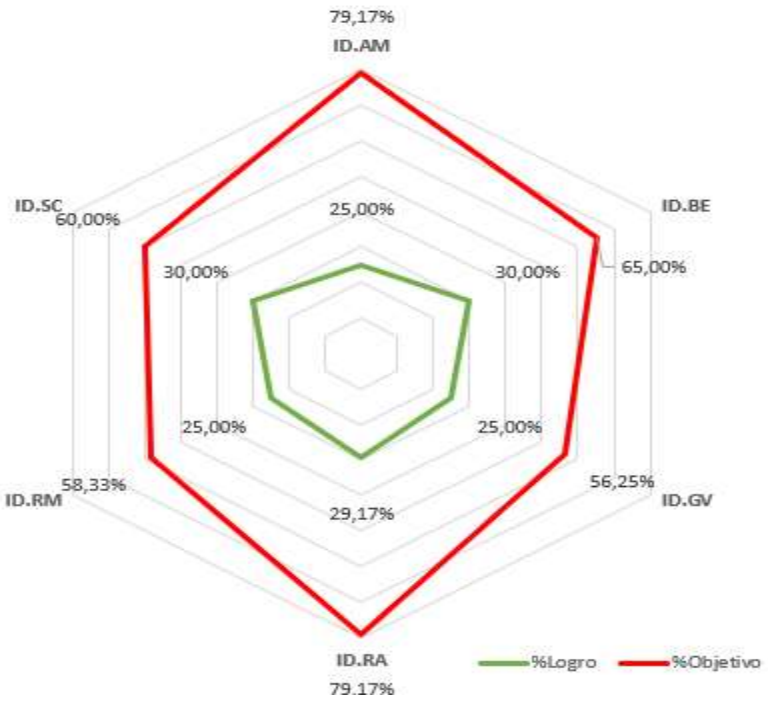
Acciones necesarias para mitigar los riesgos encontrados en la organización

3.2. Cuadro de Mando

En los gráficos 19 al 23, se determinan los estados actuales vs el estado objetivo obtenidos en el marco de trabajo de NIST, los mismos que determinan un estado Parcial que determina cada una de las subcategorías de la hoja de control NIST, que no se encontraron formalizadas y de acuerdo a su valoración .

En el Gráfico 18 determina un logro inicial en las categorías del marco de trabajo de NIST, en la categoría Identificar de la tabla 18, se determinan de las seis categorías analizadas un porcentaje promedio de logro inicial alcanzado de 27,36% y como Objetivo alcanzado de 66,32% lo que determina un porcentaje de brecha de 38,96%.

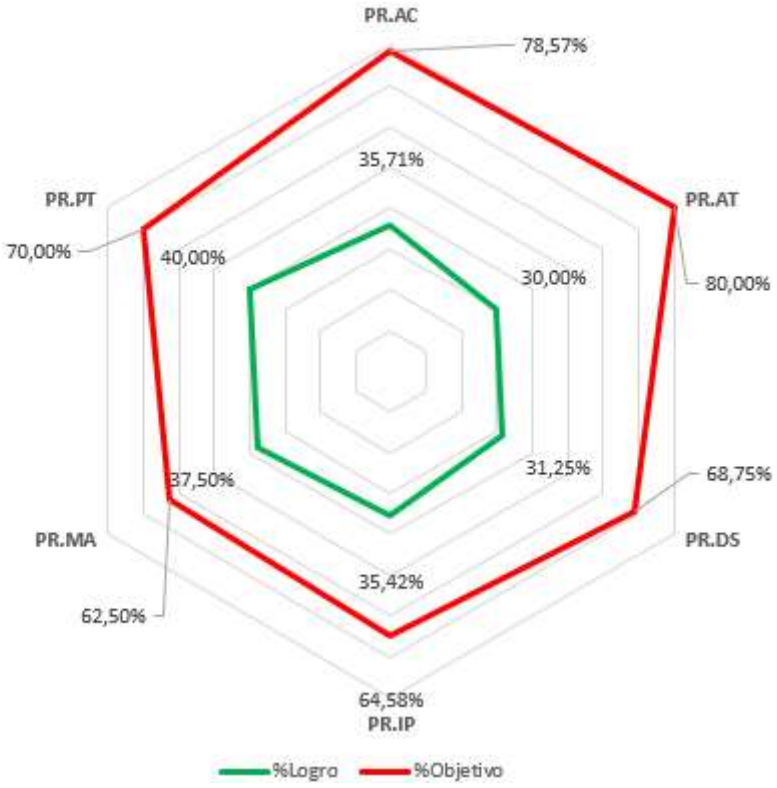
Gráfico 18: Función Identificar



Fuente: elaboración propia

En el gráfico 19 de la función Proteger del marco de trabajo de NIST, se determinó un porcentaje de logro del 34,98% y un objetivo de 70,73% los cual determinó una brecha de 35,75%, como lo determina el cuadro de mando de la función Proteger.

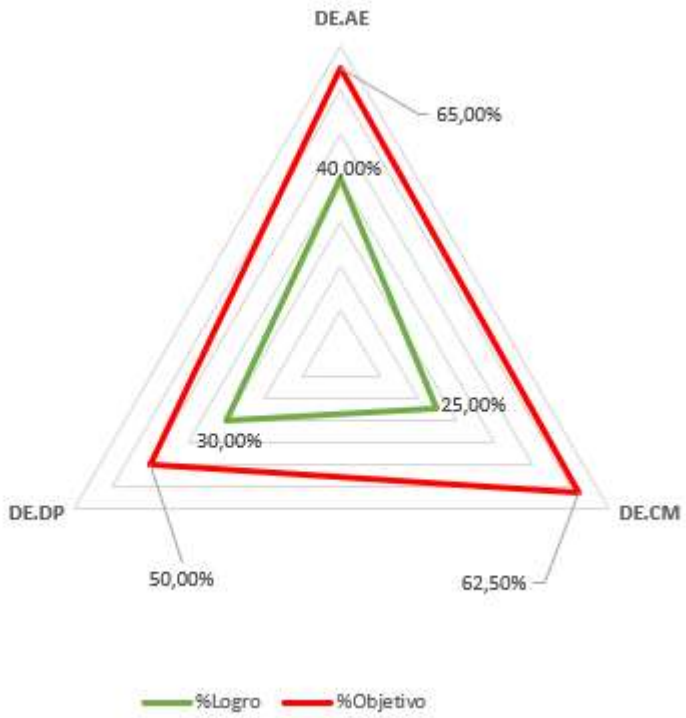
Gráfico 19: Función Proteger



Fuente: elaboración propia

En el Gráfico 20 de la función Detectar, se analizaron tres categorías las cuales, nos dan como resultado de logro inicial 31,67% y como perfil objetivo 59,17, se obtiene una brecha en esta función de 27,50%.

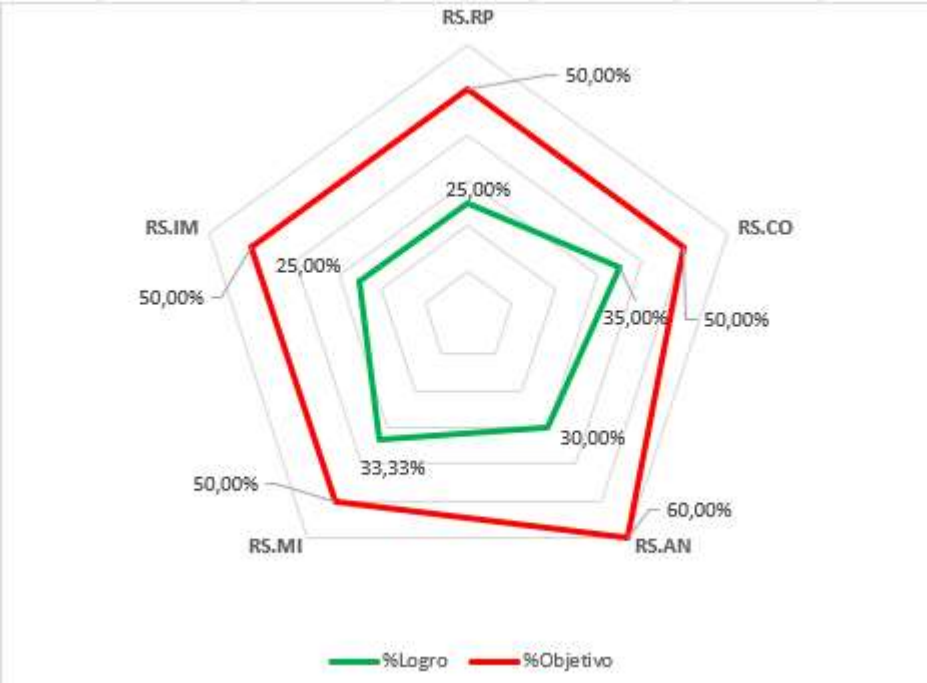
Gráfico 20: Función Detectar



Fuente: elaboración propia

En las 5 categorías analizadas de la función responder del marco de trabajo de NIST, se obtuvo un logro de 29,67% y un objetivo de 52,00% con lo cual, existe una brecha de 22,33% en esta función. Esto se visualiza en el gráfico 21.

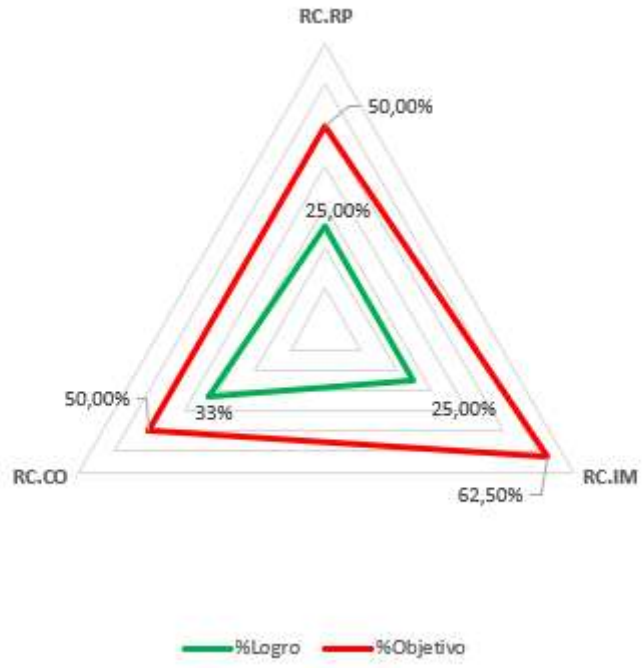
Gráfico 21: Función Responder



Fuente: elaboración propia

En la función Recuperar, se analizaron tres categorías del marco de trabajo de NIST con lo cual, se obtuvieron un logro de 27,78% y un objetivo de 54,17% con ello se determinó una brecha total para esta función del 26,39%. Esto está detallado en el gráfico 22 de la función recuperar.

Gráfico 22: Función Recuperar



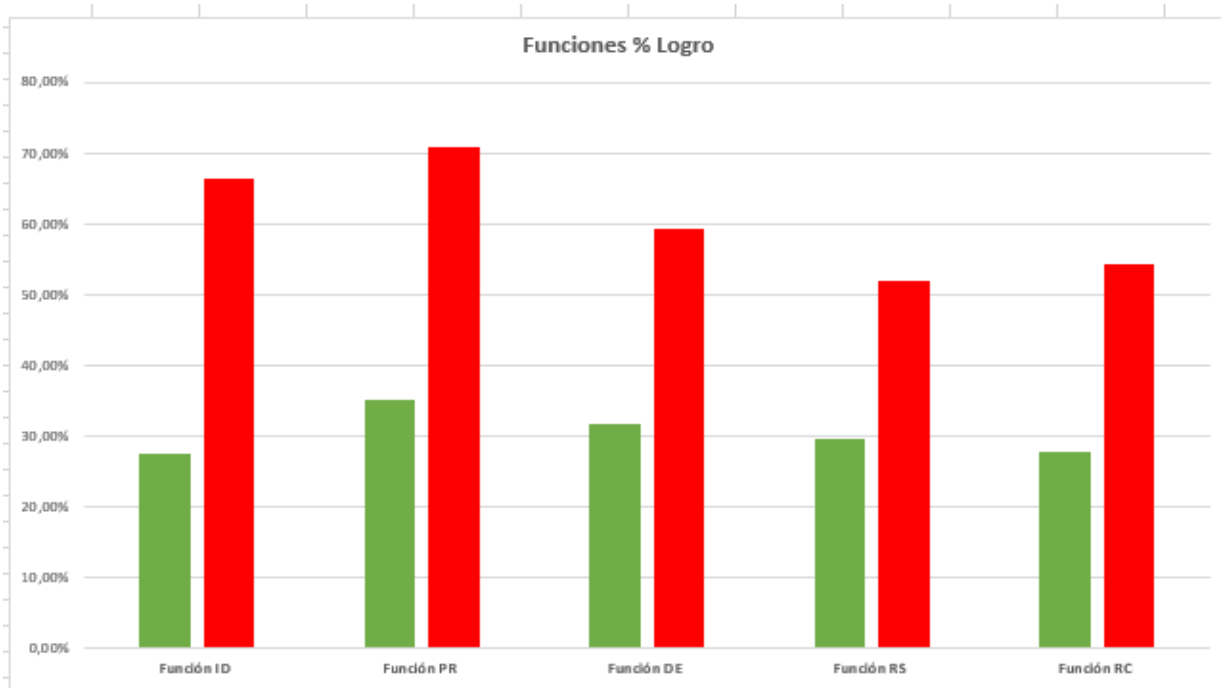
Fuente: elaboración propia

3.2.1. Perfil actual vs Logro Objetivo

En el gráfico 23 evidencia los logros y objetivos obtenidos en cada una de las funciones del marco de trabajo de NIST, con el color verde está representado el logro de cada una de las funciones y con el color rojo el objetivo de cada una de las funciones del marco de trabajo de NIST.

Del análisis gráfico realizado, se determinó que el mayor logro requerido por ser alcanzado para la organización es en la función proteger con 70,73% requerido para el cumplimiento de la organización. El siguiente logro requerido por la organización para alcanzar el logro está determinado por la función identificar con un 66,32%, para alcanzar su logro establecido.

Gráfico 23: Funciones por Logro



Fuente: elaboración propia.

CONCLUSIONES

- La implementación del Marco de Ciberseguridad de NIST, el Instituto Superior Tecnológico Sucre pudo detectar sus elementos de infraestructura crítica y con ello se pudo evaluar y mejorar las prácticas en ciberseguridad, con la utilización de la aplicación del marco de trabajo de NIST. En una fase inicial para determinar el estado actual y luego de la revisión institucional con los objetivos deseados la aplicación para obtener las brechas y con ellas desarrollar el plan de acción institucional.

- Luego de la aplicación de las dos hojas de ruta de NIST, se obtuvo que la función proteger es la de mayor porcentaje con un 70,73% en relación con las otras funciones del marco de trabajo de NIST, esto determina que la organización toma como referencia las observaciones realizadas en el plan de acción institucional entregado, para mejorar en la protección de sus activos y minimizar sus riesgos informáticos.

- El siguiente resultado encontrado es de la función Identificar con un 66,32%, que determina que se mejora en el cumplimiento de las categorías del marco de trabajo de NIST, para mejorar en la gestión de los sistemas y las instalaciones institucionales.

- Las funciones detección, responder y recuperar del marco de trabajo de NIST, están muy relacionadas por lo que se evaluó un 59,17% en la detección de eventos oportunamente, lo cual permite ser mejorado para tener una respuesta oportuna, con una correcta respuesta, se genera la recuperación en el menor tiempo posible de eventos en ciberseguridad, con ello evitar fallos en sus aplicativos webs.

- En el plan de acción, se determinaron las contramedidas necesarias para cumplir con el estándar NIST para lograr cumplir con el estado objetivo propuesto para alcanzar la meta requerida en Ciberseguridad en la institución.

RECOMENDACIONES

- Se recomienda un plan de acción basado en la guía práctica de implementación del marco de trabajo de NIST, el mismo que detalla en 7 fases la implementación correcta del marco de trabajo de NIST.

- Se recomienda el cumplimiento del plan de acción generado para llegar a cumplir con cada una de las fases determinadas por NIST para llegar al estado objetivo deseado en futuros niveles de implementación del marco de trabajo de NIST.

- Se determinaron los logros de alto riesgo para que la seguridad de los sistemas, redes y datos sean optimizados para cumplir con el marco de trabajo de NIST y de acuerdo con los estándares que se cumplen en cada subcategoría como las determinadas por COBIT 5, ISA 62443, ISO/IEC 27001, NIST SP 800-53 Rev 4.

- Se recomienda a la organización cumplir con el plan de acción y continuar con los riesgos de mediano riesgo en la organización para el cumplimiento correcto del marco de trabajo y se cierren las brechas encontradas para el correcto funcionamiento de los sistemas, redes y datos en cuanto a prevención y mitigación de posibles vulnerabilidades a presentarse.

BIBLIOGRAFÍA

27001, I. (01 de 09 de 2005). *ISO 27001*. Obtenido de https://www.normas-iso.com/iso-27001/

27001, I. (01 de 10 de 2013). *ISO 27001 Gestión Incidentes y Mejoras de Seguridad de la Información*. Obtenido de ISO 27001: https://normaiso27001.es/a16-gestion-de-incidentes-de-la-seguridad-de-la-informacion/

27001, I. (01 de 01 de 2013). *ISO.ORG*. Obtenido de https://www.iso.org/isoiec-27001-information-security.html

3.0, M. (01 de 10 de 2012). *Magerit 3.0*. Obtenido de ccn-cert: https://www.ccn-cert.cni.es /documentos-publicos/1789-magerit-libro-i-metodo/file.html

31000:2018, I. (2018). Análisis de Riesgos ISO 31000:2018. *ISO 31000:2018*, 1-16.

800-30, S. P. (2017). Guide for Conducting NIST. *Guide for Conducting*, 4.

802.11, I. (9 de 05 de 2022). *IEEE 802.11 Wireless Local Area Networks*. Obtenido de IEEE 802.11: https:// ww w.ieee802.org/11/

David A. Franco, J. L. (2012). Metodología para la Detección de Vulnerabilidades en Redes de Datos. *Scie lo*, 2.

ECONOMISTA, E. (26 de 02 de 2019). Obtenido de https://www.eleconomista.com.mx/

FLACSO. (2017). Revista Latinoamericana de Estudios de Seguridad. *URVIO*, 88.

Forum, W. E. (23 de 09 de 2020). Obtenido de Word Economic Forum: https://e s.weforum. org/agenda/2020/09/los-beneficios-inesperados-de-la-educacion-virtual/

INCIBE. (29 de 12 de 2016). *INCIBE-Activos*. Obtenido de https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci

INCIBE. (2016). *INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA*. Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

INCIBE. (18 de 05 de 2018). *Métodos de protección de Riesgos*. Obtenido de https://www.incibe.es/

ISACA. (01 de 01 de 2019). *COBIT5.* Obtenido de ISACA COBIT: https://w ww.isaca.org/resources/cobit/cobit-5#sort=relevancy

Julio Cesar Herrera, E. F. (2017). Método Científico y la investigación. *Ciencias Químicas*, 14.

MICRO, T. (23 de 02 de 2021). *TREND MICRO*. Obtenido de https://www.tr endmicro.com/vinfo/es/security/research-and-analysis/threat-reports/roundup/a-constant-state-of-flux-trend-micro-2020-annual-cybersecurity-report

NIST. (01 de 08 de 2006). *NIST Guía para la integración de técnicas forenses en la respuesta*. Obtenido de NIST: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

NIST. (01 de 09 de 2011). *NIST Monitoreo Continuo de Seguridad de la Información para Sistemas Organizacionales*. Obtenido de NIST: https://nv lpubs.nist.gov/nis tpubs/Legacy/SP/nistspecialpublication800-137.pdf

NIST. (01 de 08 de 2012). *NIST Guía de manejo de incidentes de seguridad Informática*. Obtenido de NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST. (01 de 07 de 2012). *NIST Guide to Intrusion Detection and Prevention Systems*. Obtenido de NIST: https://csrc.nist.gov/CSRC/media/Publications/sp/800-94/rev-1/draft/documents/draft_sp8 00-94-rev1.pdf

NIST. (01 de 07 de 2013). *NIST Guía para prevención y manejo de incidentes de malware para computadoras de escritorio y portátiles*. Obtenido de NIST: https: //nvlp ubs.nist. gov/nist pubs/SpecialPublications/NIST.SP.800-83r1.pdf

NIST. (22 de 12 de 2016). *NIST Guía para la recuperación de eventos de ciberseguridad*. Obtenido de NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

NIST. (01 de 04 de 2018). Obtenido de https://www.nist.gov/cyberframework

NIST. (19 de 10 de 2018). *NIST Wireless Networks*. Obtenido de NIST: https://nvl pubs.nist.g ov/nistpubs /Legacy/SP/nistspecialpublication800-48r1.pdf

NIST. (21 de febrero de 2019). *NIST Universidad de Chicago*. Obtenido de https://w ww.nist.go v/cyberframework/success-stories/university-chicago

NIST. (21 de 02 de 2019). *NIST Universidad de Pittsburgh*. Obtenido de https://www.nis t.gov/cyberframework/success-stories/university-pittsburgh

NIST. (21 de 02 de 2020). *NIST 800-171*. Obtenido de https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

NIST. (01 de 03 de 2020). *NIST Guideline for Using Cryptographic Standards in the Federal Government*. Obtenido de NIST: https://doi.org/10.6028/NIST.SP.800-175Br1

Rev.2, N. S.-5. (10 de 12 de 2020). *NIST*. Obtenido de NIST: https://csrc.nis t.gov/publicatio ns/deta il/sp /800 -55/rev-2/draft

Rubén Darío Laverde Castillo, M. H. (31 de 12 de 2020). *Centro de Investigación Avenir*. Obtenido de https://fundacionavenir.net/revista/index.php/avenir/article/view/106/60

SUCRE, I. (2020). Rendición de Cuentas 2020. 11-30.

UNESCO. (02 de 04 de 2019). *UNESCO*. Obtenido de https://www.iesalc.unesco.org/2020/04/02/el-coronavirus-covid-19-y-la-educacion-superior-impacto-y-recomendaciones/

UNESCO. (12 de 01 de 2021). *UNESCO*. Obtenido de https://es.unesco.org/

ANEXOS

Anexo 1: Encuesta Departamentos Identificación de Riesgos

INSTITUTO SUPERIOR TECNOLOGICO SUCRE

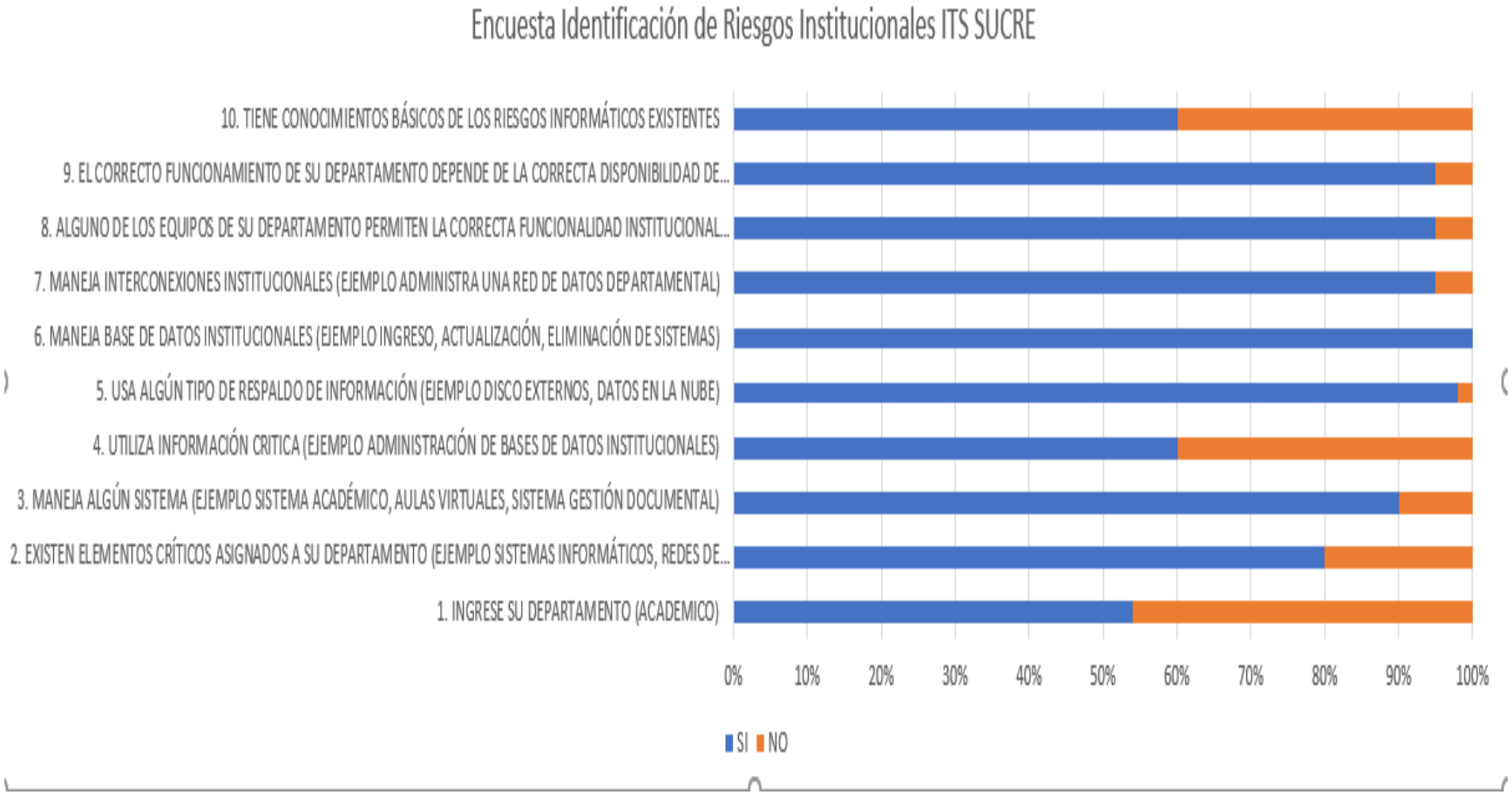
QUITO - ECUADOR

ENCUESTA IDENTIFICACION DE RIESGOS INSTITUCIONALES

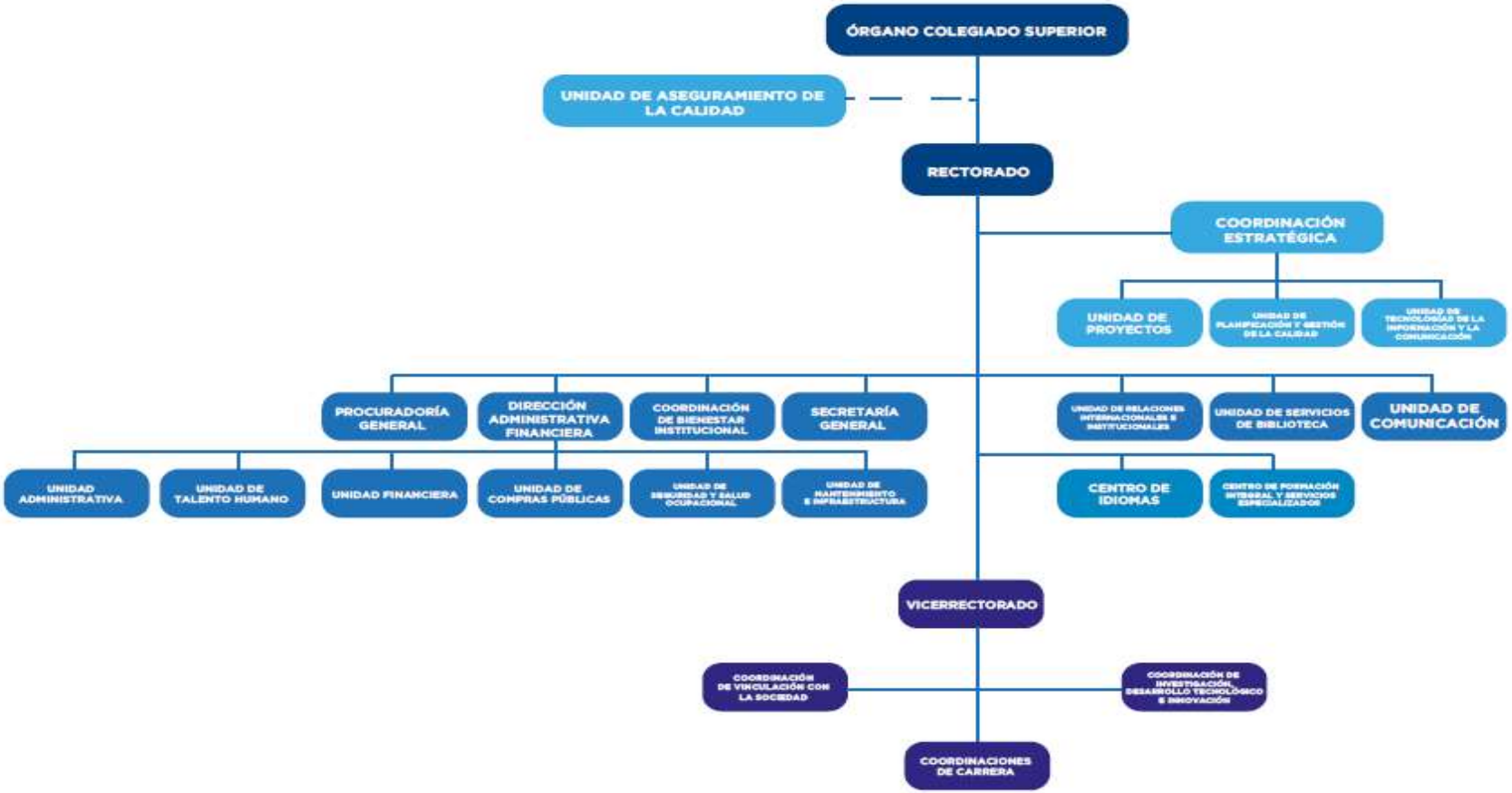
Fecha:

	Pregunta	respuesta	
1	Ingrese su departamento		
2	Existen elementos críticos asignados a su departamento (Ejemplo Sistemas Informáticos, redes de computadoras, Almacenamiento de información)	SI☐	NO☐
3	Maneja algún sistema institucional(Ejemplo Sistema Académico, Aulas Virtuales, Sistema Gestión Documental)	SI☐	NO☐
4	Utiliza información crítica(Ejemplo Administración de Bases datos institucionales)	SI☐	NO☐
5	Usa algún tipo de respaldo de información(Ejemplo Discos externos, Datos en la nube)	SI☐	NO☐
6	Maneja base de datos institucionales(Ejemplo Ingreso,actualización,eliminación de información de sistemas)	SI☐	NO☐
7	Maneja interconexiones institucionales(Ejemplo Administra una red de datos departamental)	SI☐	NO☐
8	Alguno de los equipos de su departamento permiten la correcta funcionalidad institucional(Ejemplo Servidor o equipo de manejo de respaldos)	SI☐	NO☐
9	El correcto funcionamiento de su departamento depende de la correcta disponibilidad de aplicaciones institucionales	SI☐	NO☐
10	Tiene conocimientos básicos de los riesgos informáticos existentes	SI☐	NO☐

Anexo 2. Encuesta Identificación de Riesgos Institucionales ITS SUCRE.



Anexo 3: Organigrama ITS SUCRE


ÓRGANO COLEGIADO SUPERIOR
UNIDAD DE ASEGURAMIENTO DE LA CALIDAD
RECTORADO
COORDINACIÓN ESTRATÉGICA
UNIDAD DE PROYECTOS
UNIDAD DE PLANIFICACIÓN Y GESTIÓN DE LA CALIDAD
UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN
PROCURADORÍA GENERAL
DIRECCIÓN ADMINISTRATIVA FINANCIERA
COORDINACIÓN DE BIENESTAR INSTITUCIONAL
SECRETARÍA GENERAL
UNIDAD DE RELACIONES INTERNACIONALES E INSTITUCIONALES
UNIDAD DE SERVICIOS DE BIBLIOTECA
UNIDAD DE COMUNICACIÓN
UNIDAD ADMINISTRATIVA
UNIDAD DE TALENTO HUMANO
UNIDAD FINANCIERA
UNIDAD DE COMPRAS PÚBLICAS
UNIDAD DE SEGURIDAD Y SALUD OCUPACIONAL
UNIDAD DE MANTENIMIENTO E INFRAESTRUCTURA
CENTRO DE IDIOMAS
CENTRO DE FORMACIÓN INTEGRAL Y SERVICIOS ESPECIALIZADOS
VICERRECTORADO
COORDINACIÓN DE VINCULACIÓN CON LA SOCIEDAD
COORDINACIÓN DE INVESTIGACIÓN, DESARROLLO TECNOLÓGICO E INNOVACIÓN
COORDINACIONES DE CARRERA