

IMPLEMENTAR UN PROCESO DE GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD
CON BASE EN LA NORMA ISO/IEC 27035:2023, NIST 800-61 REV-2 Y LA GUÍA
DEL MINTIC PARA LA GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD EN
EL INSTITUTO TOLIMENSE DE FORMACIÓN TÉCNICA PROFESIONAL (ITFIP).

ANDRES FELIPE CADENA INFANTE
HOLBER STEVEN HERNÁNDEZ GONZÁLEZ

UNIVERSIDAD PILOTO DE COLOMBIA.
MAESTRÍA EN SEGURIDAD INFORMÁTICA Y DE LAS COMUNICACIONES.
BOGOTÁ D.C
2026

IMPLEMENTAR UN PROCESO DE GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD
CON BASE EN LA NORMA ISO/IEC 27035:2023, NIST 800-61 REV-2 Y LA GUÍA
DEL MINTIC PARA LA GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD EN
EL INSTITUTO TOLIMENSE DE FORMACIÓN TÉCNICA PROFESIONAL (ITFIP).

ANDRES FELIPE CADENA INFANTE
HOLBER STEVEN HERNÁNDEZ GONZÁLEZ

TRABAJO DE GRADO PARA OPTAR POR EL TITULO DE MAESTRIA EN SEGURIDAD
INFORMATICA Y DE LAS COMUNICACIONES

DIRECTOR
ALVARO ESCOBAR

UNIVERSIDAD PILOTO DE COLOMBIA.
MAESTRÍA EN SEGURIDAD INFORMÁTICA Y DE LAS COMUNICACIONES.
BOGOTA D.C
2026

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Bogotá D.C., Julio del 2026

Resumen

El proyecto está enfocado a la implementación de un proceso de gestión de incidentes de ciberseguridad en el Instituto Tolimense de Formación Técnico Profesional (ITFIP) basado en tres referentes como lo son la ISO 27035:2023, la NIST 800-61 Rev2 y la Guía de gestión de incidentes propuesta por el MINTIC para entidades públicas de academia como es el caso del ITFIP, por medio de estas definiciones de buenas prácticas se hace un diseño metodológico de todo el proceso en la universidad, para ser presentado ante los directivos y posteriormente hacer todo el proceso de implementación con el acompañamiento del área de Tecnología de la Universidad.

Este proceso permitirá definir todo el flujo y las fases que debe tener un incidente de seguridad, definir matrices de escalamiento, roles y responsabilidades, para que el personal del ITFIP pueda actuar de manera idónea ante algún tipo de incidente de seguridad en los diferentes sistemas de información. Adicional a esto se definirán todas las herramientas asociadas para el desarrollo de estas actividades como lo son formatos, instructivos, bitácoras y recomendar algunos ajustes y aprovechar las herramientas tecnológicas actuales.

Finalmente se realizará un plan de concienciación que permita dar a conocer a toda la institución educativa la inclusión del proceso, como actuar, reportar y mitigar las diferentes anomalías que se lleguen a presentar, generando algunas pruebas para detectar el tiempo de respuesta y concientizar al alumnado sobre este tema.

Tabla de Contenidos

v

1.	TITULO	32
2.	PLANTEAMIENTO DEL PROBLEMA	32
3.	JUSTIFICACIÓN	36
4.	OBJETIVOS	38
4.1.	OBJETIVO GENERAL	38
4.2.	OBJETIVOS ESPECÍFICOS	38
5.	MARCO TEÓRICO.....	40
5.1.	SISTEMA DE GESTIÓN DE INCIDENTES.	40
5.2.	GESTIÓN DE INCIDENTES.....	40
5.3.	¿CUÁLES SON LOS BENEFICIOS DE UN SISTEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD Y CIBERSEGURIDAD?	41
5.4.	VALOR AGREGADO AL ITFIP POR IMPLEMENTAR UN SISTEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD Y CIBERSEGURIDAD.	42
5.4.1.	Conceptos.....	43
5.4.2.	NIST.....	47
5.4.3.	ISO 27035:2023	50
5.4.4.	Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del MinTIC.....	51
5.4.5.	CIS control V8 CSC17 - Gestión de Respuesta a Incidentes.....	55
5.4.6.	ISO27001:2022 – Apartado Gestión de Incidentes.	58
5.4.7.	Comparación de marcos de Referencia.....	59
6.	MARCOS DE REFERENCIA.....	62

6.1.	¿QUIÉN ES EL ITFIP?	62vi
6.1.1.	Misión del ITFIP	63
6.1.2.	Visión del ITFIP	64
6.1.3.	Servicios del ITFIP	64
6.1.4.	Organigrama del ITFIP	65
7.	Marco Legal	68
8.	MARCO TECNOLÓGICO	72
9.	DISEÑO METODOLÓGICO.....	77
9.1.	ESTADO ACTUAL DE LA ENTIDAD ITFIP FRENTE AL PROCESO DE GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD CON BASE EN LAS NORAMAS TECNICAS DEFINIDAS	84
9.1.1.	Análisis mapa de procesos del ITFIP	85
9.1.2.	Identificar donde se incluirá el proceso de gestión de incidentes de ciberseguridad de acuerdo con el análisis realizado.....	86
9.1.3.	GAP (Análisis de brecha)	87
9.1.3.2.	Nivel de Cumplimiento	93
9.1.4.	Conclusiones.	93
9.2.	DISEÑO DEL PROCESO DE GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD PARA LA ENTIDAD ITFIP MEDIANTE LOS MODELOS Y FRAMEWORK DE BUENAS PRÁCTICAS QUE PROPONE LA ISO 27035:2023, LA NIST 800-61 REV-2 Y LA GUÍA DE GESTIÓN DE INCIDENTES DEL MINTIC	94
9.2.1.	Documentarse sobre los frameworks ISO27035:2022, NIST 800-61 Rev-2 y la Guía de Gestión de incidentes de seguridad del MINTIC	96

9.2.2. Generar entrevistas con las áreas que deberían estar a cargo del proceso de	vii
gestión de incidentes	96
Área o Cargo	97
Rol en el proceso.....	97
Tecnología.....	97
Contención y soporte en incidentes	97
Analista de Soporte	97
Recepción de reportes y primeros diagnósticos.....	97
Oficial de Seguridad	97
Coordinación Gestión de Incidentes	97
Coordinador de Redes.....	97
Análisis de tráfico y mitigación en la red	97
Asesor Legal- Gestión administrativa.....	97
Evaluación legal y soporte ante incidentes con impacto regulatorio.....	97
Analista de Riesgos- Calidad	97
Identificación de impacto y priorización de riesgos	97
Coordinadora de Comunicaciones	97
Manejo de la comunicación interna y externa	97
RRHH – Gestión Administrativa.....	97
Gestión de incidentes relacionados con personas internas	97
Gestión Administrativa - Continuidad.....	97
Apoyo en activación de planes de recuperación	97

9.2.3.	Verificar si se cuenta con la política o lineamientos asociados a la gestión de incidentes y actualizar o acompañar en su definición.....	viii 100
9.2.4.	Propuesta del Diseño de la Gestión de Incidentes de Ciberseguridad de la ITFIP por etapas.	102
9.2.5.	Propuesta de los roles, responsabilidades y personal necesario por la atención de los incidentes de seguridad y Ciberseguridad.....	104
9.2.6.	Propuesta de la matriz de escalamiento: interna y externa.	107
9.2.7.	Propuesta de documentos clave que apoyan el proceso de gestión de incidentes. .	108
9.2.8.	Proponer de métricas e indicadores de referencia, para la mejora continua.	111
9.2.9.	Presentar diseño y propuesta a los directivos y responsables del proceso de gestión de incidentes del ITFIP.	113
9.2.10.	Conclusiones	114
9.3.	PROCESO DE GESTION DE INCIDENTES DE CIBERSEGURIDAD PARA LA ENTIDAD ITFIP	115
9.3.1.	Definir formalmente las etapas de implementación que harán parte del proceso de gestión de incidentes de ciberseguridad. (Implementación).	117
9.3.2.	Formalizar la matriz de roles y responsabilidades del proceso de gestión de incidentes de ciberseguridad. (Implementación)	118
9.3.3.	Formalizar e implementar la matriz de escalamiento interna y externa que fueron definidas para el proceso de gestión de incidentes de ciberseguridad, para su publicación. (Implementación).	119

9.3.4.	Formalizar e implementar los documentos propuestos para apoyar el proceso de gestión de incidentes de ciberseguridad, incluyéndolos en el sistema de calidad para su seguimiento. (Implementación).	ix 120
9.3.5.	Implementar y formalizar el reporte de métricas definidas para medir el proceso de gestión de ciberseguridad, con los responsables de su medición y reporte. (Implementación).	124
9.3.6.	Generar acta de cierre de implementación del proceso de gestión de incidentes de ciberseguridad para su publicación y cumplimiento. (Implementación).	125
9.3.7.	Conclusiones.	125
9.4.	PLAN DE CONCIENTIZACIÓN DE LA GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD.	127
9.4.1.	Propuesta Plan de Concienciación	127
9.4.2.	Objetivos	129
9.4.3.	Alcance	129
9.4.4.	Público Objetivo	129
9.4.5.	Temas	130
9.4.6.	Material de Apoyo	131
9.4.7.	Responsables	132
9.4.8.	Comunicación	132
9.4.9.	Ejecución	133
9.4.10.	Medición	134
9.4.11.	Anexos Plan de concienciación	135

9.4.12.	Crear campañas de concienciación para todo el alumnado, personal administrativo x y docente del ITFIP sobre como reportar y actuar ante un incidente de ciberseguridad.	138
9.4.13.	Dar recomendaciones y sugerencias sobre la importancia de la seguridad y ciberseguridad a nivel institucional.	138
9.5.	ANALISIS DE RESULTADOS	141
9.5.1.	Conclusión de resultados del antes y después del proceso de gestión de incidentes de Ciberseguridad.	141
10.	CONCLUSIONES	146
11.	LECCIONES APRENDIDAS	148
12.	TRABAJO FUTURO.....	150
13.	AGRADECIMIENTOS	151
14.	BIBLIOGRAFÍAS	152
	Referencias.....	152
	ANEXO A.....	156
14.1.	GAP.....	156
	ANEXO B.....	166
14.2.	Check de Incidentes	166
14.3.	Formato para reporte de Incidentes de Ciberseguridad	170
14.4.	Formato de resolución rápida para incidentes de Ciberseguridad	174
14.5.	Formato Verificador de servicios post-Incidente de Ciberseguridad	177
14.6.	Bitácora de Incidentes de Ciberseguridad.....	180
14.7.	Formato de Comunicación de Incidentes de Ciberseguridad.	182
14.8.	Formato Matriz de Contactos de emergencia	188

ANEXO C	191xi
14.9. Guía escenario general	191
14.10. Guía casos – Respuesta a incidentes	191
14.11. Guía - Casos de Intrusión.....	193
14.12. Guía – Casos de Denegación de servicios.	196
14.13. Guía – Casos de Código Malicioso.....	201
14.14. Guía – Casos identificar posible amenaza.	205
ANEXO D	208
14.15. Perfiles Sugeridos	208
14.15.1. Perfil Director	208
14.15.2. Perfil Profesional	215
14.15.3. Perfil Analista	220
14.16. Presupuesto	226
ANEXO E	227
14.17. Gestión de Incidentes de Ciberseguridad.....	227
14.17.1. Introducción	228
14.17.2. Descripción	229
14.17.3. Objetivo.....	230
14.17.4. Alcance	230
14.17.5. Referencia	230
14.17.6. Guías	231
14.17.7. Términos y Definiciones.....	231
14.17.8. Clasificación de Incidentes de Ciberseguridad/Seguridad.....	232

14.17.9.	Tipo de Amenaza	232xii
14.17.10.	Origen de la amenaza.....	233
14.17.11.	Categoría	233
14.17.12.	Perfil de usuario	233
14.17.13.	Requerimientos legales.	233
14.17.14.	Taxonomía de clasificación los incidentes de ciberseguridad/seguridad.	234
14.17.15.	CSIRT	241
14.17.16.	Estructura del CSIRT	241
14.17.17.	Líder CSIRT.....	241
14.17.18.	Roles y Responsabilidades.....	242
14.17.19.	CISO – Responsable de Ciberseguridad/Seguridad -Responsable Grupo Atención a Incidentes.	242
14.17.20.	Director de TI.....	243
14.17.21.	Líder de Mesa de Ayuda.....	244
14.17.22.	Administrador de la Plataforma / Aplicación	244
14.17.23.	Usuario Final.....	245
14.17.24.	Responsable Jurídico.	245
14.17.25.	Líder de Comunicaciones.	245
14.17.26.	Etapas del Incidente	246
14.17.27.	Prevención y preparación.....	246
14.17.28.	Detección	248
14.17.29.	Contención Erradicación y Recuperación.....	249
14.17.30.	Actividades Post incidente-Lecciones Aprendidas	252

14.17.31.	Diagrama Etapas Definidas para la Gestión de Incidentes de Ciberseguridad.	xiii
		254
14.17.32.	Medición	255
14.17.33.	Comunicación del Incidente	257
14.17.34.	Interna	257
14.17.35.	Externa	260
14.17.36.	Control de Cambios	262
ANEXO F		265
14.18.	Manual de Procedimiento	265
14.18.1.	Flujo del incidente.....	265
14.18.2.	Flujograma Gestión eventos de Ciberseguridad y Seguridad	32
14.18.3.	Sub-proceso – Recepción del Evento	32
14.18.4.	Sub-proceso del Comité de Crisis del incidente de Ciberseguridad	33
14.18.5.	Sub-proceso de Contención	35
14.18.6.	Sub-proceso Erradicación	38
14.18.7.	Sub-proceso Recuperación.....	40
14.19.	Niveles de atención de un incidente de ciberseguridad.	42
14.20.	Registro de eventos	44
14.21.	Registro de Incidentes en el Sistema.	48
14.22.	Gestión de equipo de respuesta.....	51
ANEXO G		¡Error! Marcador no definido.
14.23.	Acta: Presentación del Diseño de Gestión de Incidentes de Ciberseguridad....	¡Error!
		Marcador no definido.

ANEXO H..... **¡Error! Marcador no definido.**^{xiv}

14.24. Acta de implementación del proceso de gestión de incidentes de ciberseguridad de la
ITFIP. **¡Error! Marcador no definido.**

Tabla de Tablas

Tabla 1 Controles Gestión de Incidentes ISO27001:2022.....	58
Tabla 2 Comparación marcos de referencia.....	59
Tabla 3 Normativas.....	68
Tabla 4 Marco Metodológico.....	78
Tabla 5 Actividades del Proyecto	85
Tabla 6 Dominios Evaluados en el GAP	87
Tabla 7 Preguntas del GAP.....	88
Tabla 8 Propuesta de cargos	97
Tabla 9 Indicador de Respuesta	111
Tabla 10 Indicador de Cantidad de Incidentes.....	112
Tabla 11 Indicador Falsos Positivos	113
Tabla 12 Etapas de Implementación	117
Tabla 13 Capacitaciones de concientización	133
Tabla 14 Indicador de Efectividad -concientización	134
Tabla 15 Indicador de Participación -concientización.....	135
Tabla 16 Definición de pesos por dominio	142
Tabla 17 Nivel de cumplimiento.....	143
Tabla 18 GAP	156
Tabla 19 Lista de Chequeo	166

Tabla de Ilustraciones

xvi

Ilustración 1 Fases de Proceso Incidentes NIST	47
Ilustración 2 Ciclo de vida de la gestión y respuesta a un incidente de seguridad	53
Ilustración 3 Salvaguardadas de Gestión de Incidentes CSC17 CIS V8	56
Ilustración 4 Salvaguardadas de Gestión de Incidentes CSC17 CIS V8 parte 2	57
Ilustración 5 Organigrama ITFIP	65
Ilustración 6 Organigrama Directivo ITFIP	66
Ilustración 7 Mapa de Procesos ITFIP	67
Ilustración 8 Arquitectura de Referencia	76
Ilustración 9 Mapa de Procesos	86
Ilustración 10 Diseño del Proceso Gestión de incidentes de Ciberseguridad	103
Ilustración 11 Estructura Actual	105
Ilustración 12 Estructura Propuesta	106
Ilustración 13 Infografía según NIST	136
Ilustración 14 Pieza Informativa	137
Ilustración 15 Pieza Informativa del Proceso	137
Ilustración 16 Pieza Informativa	138
Ilustración 17 Estado antes y después	141
Ilustración 18 Resultados	144
Ilustración 19 Proceso de Gestión de Incidentes de Ciberseguridad	32
Ilustración 20 Subproceso Recepción del evento	32
Ilustración 21 Subproceso Comité de Crisis	35

Ilustración 22 Subproceso Contención	37xvii
Ilustración 23 Subproceso Erradicación	39
Ilustración 24 Subproceso Erradicación	41
Ilustración 25 Subproceso Gestión del evento	47

1. TITULO

Implementar un proceso de gestión de incidentes de ciberseguridad con base en la norma ISO/IEC 27035:2023, NIST 800-61 Rev. 2 y la Guía del MinTIC para la gestión de incidentes de ciberseguridad en el Instituto Tolimense de Formación Técnica Profesional (ITFIP).

2. PLANTEAMIENTO DEL PROBLEMA

El Instituto Tolimense de Formación Técnica Profesional (ITFIP) es una institución educativa publica de nivel superior ubicada en el Espinal Tolima, la cual cuenta con una planta de 103 personas, donde hay personal docente y administrativo más el personal que labora por prestación de servicios de los cuales la mayoría están en el área de Tecnología, adicional a esto cuenta con más de 1500 estudiantes matriculados, en general estamos hablando de más de 1600 usuarios que se conectan a la red del ITFIP, sin contar los usuarios invitados y temporales.

EL ITFIP cuenta con varios sistemas de información, página WEB <https://itfip.edu.co> y algunos servicios expuestos a internet, lo cual lo hace visible ante la red de internet en general, donde puede ser objetivo de diferentes tipos de ataques como suplantaciones, denegación de servicios, entre otros, dirigidos a los activos de información.

De acuerdo con el acercamiento realizado al ITFIP, se identificó su esquema organizacional, Core de negocio, y sus clientes (estudiantes), también se validó las

certificaciones con las que cuenta, en este caso el estándar ISO 9001 enfocada a todo el sistema de gestión de calidad.

De acuerdo a lo mencionado anteriormente, se identificó debilidades al no tener implementado un estándar de seguridad como referencia al framework de buenas prácticas como son la ISO 27001:2013-2022, CIS control o la NIST, en donde hay controles asociados a la gestión de incidentes; adicional a esto en los procesos enmarcados por la universidad no hay lineamientos, políticas de gestión, ni procesos en donde se relacionen guías o playbooks de cómo gestionar los incidentes de ciberseguridad en el ITFIP.

Otra debilidad es que en su esquema organizacional no hay un área de seguridad independiente con los roles adecuados para la gestión de incidentes, ni responsabilidades en este frente, toda esta responsabilidad recae sobre la Dirección de Tecnología. Sus recursos de planta son limitados y los demás son por medio de prestación de servicios, en donde vemos una gran oportunidad de mejora que permite apalancar más la inclusión y estructuración de implementar el proceso de gestión de incidentes de ciberseguridad que permita al ITFIP tener bases sólidas y un esquema de respuesta ante una posible amenaza que comprometa alguno de sus activos de información.

En las entrevistas con los colaboradores del ITFIP, no se cuenta con un proceso de auditoría de seguridad a los procesos tecnológicos, son más enmarcados al área administrativa, por lo cual identificamos otra oportunidad de mejora que es definir un esquema de auditoría que permita a la universidad lograr evaluar los procesos actuales y esté nuevo que se propondrá sobre la gestión de incidentes de ciberseguridad, además de dar capacitaciones que les permita tener una visión más amplia frente a temas seguridad

enmarcado a lo que se propone en la guía de gestión de incidentes y seguridad que entrega el MinTIC (MinTIC, 2021) para todas las entidades del gobierno.

Frente al contexto descrito anteriormente, se deben trabajar en las siguientes oportunidades de mejora:

- Se debe definir un plan de capacitación para el personal de TI para que pueda emplear buenas prácticas frente a los procesos de tecnología, técnicos y de la operación que ayuden a identificar posibles amenazas o eventos que puedan llegar a materializar el riesgo y generar un incidente de seguridad que de llegar materializarse pueden generar un gran impacto al ITFIP a nivel reputacional, económico y hasta disciplinario.
- Se debe definir y diseñar un proceso de gestión de incidentes de ciberseguridad alineado al MINTIC (MINTIC, 2016), y basado en los framework de la NIST 800-61 Rev-2 y la ISO 27035:2022 parte 1 y 2, en donde se alinee con los objetivos de negocio del ITFIP permitiendo tener un esquema de respuesta idóneo ante alguna amenaza que impacte a la universidad.
- Se debe definir roles y responsabilidades para los funcionarios de TI que harán parte del proceso de respuesta a incidentes de ciberseguridad, donde permita tener una matriz de escalamiento y reportes a los CSIRT gobierno, Centro Cibernético policial, COLCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) y demás entes que apoyen estos procesos para recibir apoyo recomendaciones y boletines que ayuden a estar al tanto de las amenazas actuales y aplicar medidas de contención.

De todas las oportunidad de mejora identificadas y de lo propuesto a nivel general surge la siguiente pregunta de investigación: **¿Como se puede definir e implementar un proceso de gestión de incidentes de ciberseguridad alineado a las políticas de gobierno que debe cumplir el ITFIP, para adoptar buenas prácticas, tener un esquema organizacional adecuado, definir roles y responsabilidades, además de contar con capacitación adecuada a todo el personal y clientes que hacen parte de la institución con el fin de tomar decisiones adecuadas y contener cualquier tipo de amenaza que comprometa la confidencialidad, integridad y disponibilidad de la información ?**

Al lograr abarcar esta problemática y aplicar las oportunidades de mejora, permitirá a la institución educativa dar cubrimiento a varios temas normativos y aplicar buenas prácticas que ayudaran a mejorar sus procesos y la concienciación de las partes interesadas en la mejora continua de la seguridad, que es uno de los factores más importantes frente al manejo de información, al abordar cada uno de los hitos definidos, se logrará cubrir las necesidades ayudando a que se tenga buena toma de decisiones y el personal sepa que hacer, como actuar y como reportar cualquier amenaza o factor que vulnere los pilares de seguridad y ciberseguridad de la información. Por medio de los aportes de investigación aplicada que se entregaran en este proceso, se dará cubrimiento a las necesidades actuales del ITFIP frente a la gestión de incidentes.

3. JUSTIFICACIÓN

Uno de los propósitos de gran interés de las entidades empresariales es fortalecer sus sistemas informáticos más seguros y confiables, de forma que puedan operar y dar soportabilidad de los servicios prestados como unidad de negocio de forma segura ; esto acompañado antes los sucesos actuales a ataques cibernéticos, apertura de nuevas vulnerabilidades referente a los problemas o dificultades de seguridad en los recursos expuestos involucrando servicios web, servidores, puertos publicados, bases de datos, y demás; que claramente la información expuesta que circula es atractiva para los piratas informáticos que buscan atentar contra la disponibilidad, confidencialidad e integridad de los servicios ofrecidos y bajo fines delictivos para la apropiación de los datos, afectación reputacional de la organización o indisponibilidad del mismo servicio en el impacto de continuidad y operación de la entidad en el mercado. (ISACA, 2015)

Este proyecto contribuye como un plan de mejora con la concientización e importancia de la protección de los activos de la empresa sobre la seguridad de la información y la importancia de tener una adecuada gestión que permita estar alerta ante una posible amenaza a través del análisis y gestión de incidentes de seguridad (MINTIC, 2016). Por esta razón es necesario desarrollar estrategias que permitan dar el tratamiento adecuado y la capacidad de reaccionar de forma temprana ante ataques cibernéticos en la guía para localización, análisis y evaluación de vulnerabilidades e incidentes a los que puede estar expuesta la organización, que atentan contra la integridad, confidencialidad y disponibilidad de la información

Para esta situación, la compañía ve la necesidad de implementar controles y/o metodologías que permitan la gestión y control del flujo de la información, dando respuesta frente a un vector de ataque en proceso, mediante la contención, mitigación y control de este. Para esta situación, se ve la necesidad de implementar la aplicabilidad de la gestión de incidentes (MinTIC, 2021) de seguridad de la información para la infraestructura tecnológica del Instituto Tolimense de Formación Técnica Profesional (ITFIP) con base en la norma ISO/IEC 27035:2016, NIST SP 800-61 R.2, CIS V8 para conformar el grupo de respuesta a incidentes. Para la empresa es importante definir la metodología para poder priorizar estos tipos de riesgo dando un enfoque efectivo en los recursos y servicios tecnológicos a nivel de prevención, detección, remediación y respuesta.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Implementar un modelo de gestión de incidentes de ciberseguridad en la institución educativa ITFIP, aplicando los estándares de buenas prácticas ISO 27035:2023, NIST 800-61 Rev-2 y la guía de gestión de incidentes de seguridad de la información del MINTIC, frente a los lineamientos y definiciones del proceso de gestión de incidentes; ayudando a definir las matrices de escalamiento, roles y responsabilidades con todo el flujo desde el reporte (alerta-evento) o la identificación de una amenaza hasta el cierre de la acción ejecutada, permitiendo al personal del ITFIP actuar de manera oportuna ante un incidente de seguridad o ciberseguridad.

4.2. OBJETIVOS ESPECÍFICOS

Identificar si existen subprocesos de seguridad o ciberseguridad en el mapa de procesos del ITFIP en la parte tecnológica, permitiendo establecer cómo se incluirá el proceso de gestión de incidentes de ciberseguridad; generando un GAP (Análisis de brecha), para determinar que se debe tener en cuenta para la inclusión del nuevo proceso.

Diseñar y proponer un proceso de gestión de incidentes de ciberseguridad para el ITFIP mediante los modelos y framework de buenas prácticas que propone la ISO 27035:2023, la NIST 800-61 Rev-2 y la Guía de Gestión de Incidentes del MinTIC, para estructurar el proceso, guías y definiciones de la gestión de incidentes.

Implementar el proceso de gestión de incidentes de ciberseguridad con todo el flujo de trabajo, formatos, anexos, guías y definiciones de acuerdo con el diseño que adopte el ITFIP; para que el equipo de tecnología pueda actuar correctamente ante un incidente de ciberseguridad.

Capacitar el personal sugerido y el propuesto por los directivos del ITFIP en todas las fases del proceso de la gestión de incidentes de ciberseguridad, por medio de un plan de concientización, que permita a toda la institución educativa saber cómo actuar, a quien reportar y que acciones tomar ante los diferentes escenarios de un incidente de ciberseguridad.

Generar un análisis de resultados con base en la efectividad de implementar el modelo propuesto para la gestión de incidentes de ciberseguridad del ITFIP.

5. MARCO TEÓRICO

5.1.SISTEMA DE GESTIÓN DE INCIDENTES.

(ISO.ORG, 2023) Un SGISI (Sistema de gestión de incidentes de seguridad de la información) es un conjunto estructurado de procesos y herramientas diseñadas para detectar, responder, mitigar y gestionar incidentes de ciberseguridad dentro de una organización. Su objetivo principal es minimizar el impacto de los incidentes de seguridad y garantizar la continuidad del negocio.

Dentro de cualquier organización debe existir una política de gestión de incidentes que hace parte de la estrategia de la seguridad de la información; esta política debe otorgar lineamientos formales documentados para la aplicabilidad en la toma de decisiones, procesos y procedimientos que garantizan la aplicación de esta política.

5.2.GESTIÓN DE INCIDENTES.

La gestión de incidentes de seguridad de la información hace parte de la gestión de servicios de tecnologías de la información dentro de una compañía. Su principal objetivo es mantener la confidencialidad, integridad y disponibilidad de los activos de información, reduciendo al máximo el riesgo o impacto negativo que pueda materializarse para la organización. Para esta gestión el estándar internacional ISO/IEC 27035:2023 describe un enfoque estructurado y planificado para detectar, reportar y evaluar los eventos e incidentes de seguridad de la información. (ISO.ORG, 2023)

Esta guía de gestión de incidentes tomada como referencia en la NIST:

Para definir las actividades de esta guía se incorporaron componentes definidos por el NIST (NIST, 2023) alineados con los requerimientos normativos de la ISO/IEC 27035- 2023, esta misma plantea una serie de actividades en el cumplimiento con el ciclo de vida de la gestión y respuesta a incidente de seguridad de la información.

- Preparación
- Detección y análisis
- Contención, erradicación y recuperación.
- Revisión post incidente.

5.3.¿CUÁLES SON LOS BENEFICIOS DE UN SISTEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD Y CIBERSEGURIDAD?

Siguiendo la guía de las fases mencionadas anteriormente, tienen como aporte varios beneficios para la compañía; (Center for Internet Security, 2021) dentro de ellos está en el tiempo de respuesta en los incidentes, restauración ágil del sistema que como resultado es que la pérdida de información sea mínima, mejora de la gestión cuando se tiene registros de las actividades, mayor productividad y control de los procesos del sistema de información y monitoreo, mejoramiento de la productividad en la institución, cumplimiento de los niveles de servicio SLA establecidos y la optimización de los recursos disponibles.

5.4.VALOR AGREGADO AL ITFIP POR IMPLEMENTAR UN SISTEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD Y CIBERSEGURIDAD.

- Resolución rápida de problemas frente a incidentes que se presenten en la infraestructura de la organización.
- Colaboración e intercambio de conocimientos, colaboración entre equipos, Cuando se produce una interrupción del servicio, es una oportunidad para que los miembros de su equipo trabajen juntos.
- Transparencia al mantener informadas a todas las partes interesadas de la empresa, Esta transparencia fomenta la confianza entre los equipos de TI, la administración y sus clientes.
- Implementar y desarrollar herramientas internas para la escalabilidad.
- Mejoramiento de los controles y medidas de seguridad, al integrar la seguridad en el proceso de gestión de incidentes, fortalece las defensas y reduce el riesgo de amenazas cibernéticas, preservando la integridad y confiabilidad del negocio.
- Permite la identificación proactiva de modificaciones y mejoras beneficiosas del sistema.
- Notificación eficiente de los incidentes.
- Cumplimientos normativos con las entidades legales.
- Mitigación de riesgos respecto a los activos críticos de información.
- Promueve la cultura cibernética de mejora continua.

- Garantizar la efectividad de la política de seguridad y privacidad de la información.
- Mejorar los procesos y poder responder a los incidentes relacionados con la seguridad de la información de forma eficiente y efectiva.

5.4.1. Conceptos

De acuerdo con el COLCERT (Grupo de Respuestas a Emergencias Cibernéticas de Colombia) “Los ataques cibernéticos a las instituciones y organizaciones, se vienen enfocando en la explotación de vulnerabilidades conocidas, que no han sido corregidas a pesar de existir actualizaciones publicadas por los fabricantes de equipos, así mismo la obsolescencia tecnológica y aplicaciones legadas que soportan procesos misionales en entidades y privados, aumentan la superficie de exposición, estas debilidades permiten a los ciberdelincuentes ingresen a los sistemas de información e infraestructuras tecnológicas fácilmente, logrando tener acceso a los dispositivos para comprometerlos, y a la información para luego ser exfiltrada, puesta en venta y publicada en redes para iniciar campañas de desacreditación institucional” (COLCERT, 2023) Las instituciones educativas no son la excepción de los grupos de ciberdelincuentes, por esta razón se debe contar con un proceso de gestión de incidentes de ciberseguridad para actuar de manera adecuada ante estos escenarios. De acuerdo con la Guía de Gestión y clasificación de incidentes de Seguridad de la

Información (MINTIC, 2016), se debe definir modelo que permita a las entidades públicas como lo es el ITFIP contar con:

- Roles y responsabilidades para evaluar todo lo relacionado con riesgos.
- Tener gestión sobre los eventos de seguridad de la información por medio de un triage que permita hacer una clasificación sobre los eventos de seguridad.
- Evaluar y dar respuesta a los posibles eventos de seguridad de manera oportuna.
- Contar con salvaguardas que permitan minimizar la materialización de incidentes de seguridad.
- Documentar las lecciones aprendidas que deja cada uno de los incidentes de seguridad, para aprender de los comportamientos y tomar acciones futuras posibles incidentes de la misma categoría. Permitiendo mejorar las salvaguardas o controles complementarios.
- Definir mecanismos que permitan cuantificar los incidentes de seguridad, por medio de las bases de datos de conocimiento y definiendo métricas.
- Definir un procedimiento formal del reporte y escala de incidentes de seguridad.

En este espacio se tendrán en cuenta los conceptos que se desarrollarán y serán abordados a lo largo del proyecto con las temáticas de investigación definidas en la gestión de incidentes.

Se inicia con un concepto que es fundamental en todo el desarrollo de la investigación denominado “incidente de seguridad” según (Tejada, 2023), el cual menciona que un incidente de seguridad es cualquier evento que pueda afectar a la integridad, confidencialidad y disponibilidad de la información¹.

Otra definición, entregada por la ISO 27001:2013 (INCONTEC, 2013), define un incidente de seguridad es un evento no deseado o no esperado que puede comprometer significativamente las operaciones.

La (NIST, 2023) lo define como un suceso potencial, que pone en peligro la confidencialidad, integridad y disponibilidad de un sistema de información, en donde el sistema, procese, almacene o transmita que constituye a una violación o amenaza inminente de violación a la política de seguridad o demás procesos asociados.

Teniendo en cuenta las definiciones anteriores, se relacionan los demás conceptos relacionados con incidente de seguridad:

- Evento: Un evento es cualquier suceso observable en un sistema o red. (NIST, 2020)
- Confidencialidad: propiedad de que la información no se pone a disposición ni se divulga a personas, entidades o procesos no autorizados. (ISO/IEC 27000, 2018)

¹ (Tejada, 2023)

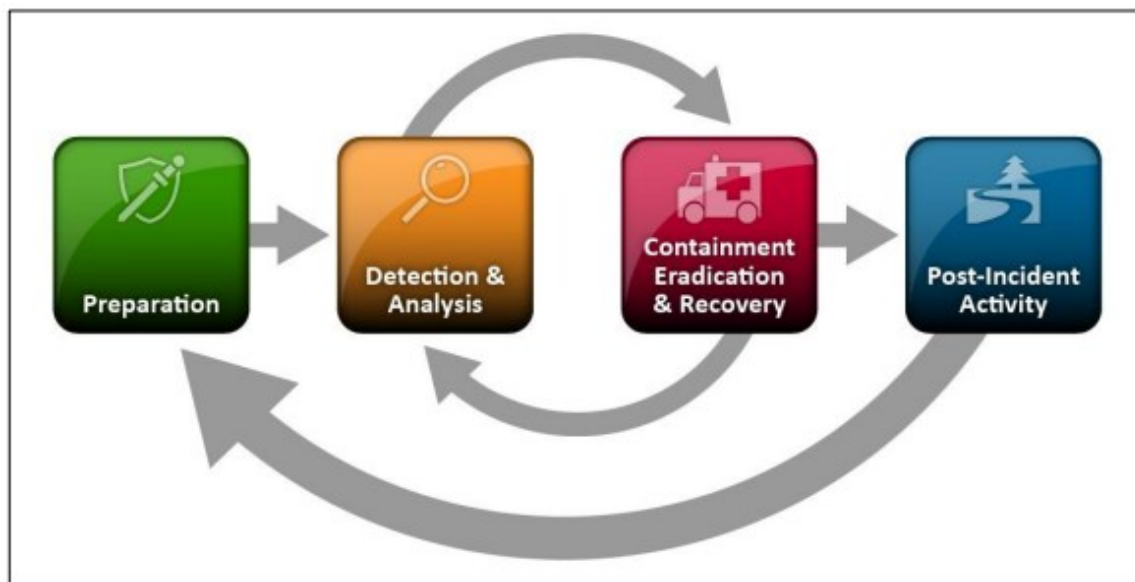
- Integridad: propiedad de exactitud e integridad. (ISO/IEC 27000, 2018)
- Disponibilidad: propiedad de ser accesible y utilizable a pedido por una entidad autorizada. (ISO/IEC 27000, 2018)
- Amenaza: Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización. (ISO/IEC 27000, 2018)
- Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una o más amenazas. (ISO/IEC 27000, 2018)
- Proceso: Conjunto de actividades interrelacionadas o que interactúan y que transforman los insumos en productos. (ISO/IEC 27000, 2018)
- Monitoreo: Determinar el estado de un sistema, un proceso o una actividad. (ISO/IEC 27000, 2018)
- Incidente de seguridad de la Información: eventos de seguridad de la información únicos o una serie de eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información. (ISO/IEC 27000, 2018)
- Ataque: intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo. (ISO/IEC 27000, 2018)

- Concienciación: Capacitar al personal de la organización en temas de seguridad de la información. (ISO/IEC 27000, 2018)
- Controles: Medidas para modificar el riesgo. (ISO/IEC 27000, 2018)

5.4.2. NIST

Por otra parte, tenemos la definición de la (NIST, 2020) en la Guía de gestión de incidentes las diferentes etapas y el ciclo de vida de una adecuada gestión de incidentes de seguridad en la ilustración 1 se identifica las fases propuestas y su relación:

Ilustración 1 Fases de Proceso Incidentes NIST



Autor: (NIST, 2020)

Tal como se muestra en la ilustración 1 se describen cada una de las fases de acuerdo con lo definido por la NIST (NIST, 2020):

- **Preparación:** Permite definir la metodología que va a ser empleada, tener capacidad de respuesta para que la organización esté preparada a atender un incidente de seguridad, pero al mismo tiempo tener la capacidad de prevenirlos, en esta etapa la NIST (NIST, 2020), logra dar todos los alcances de cómo prepararse ante un incidente de seguridad.
- **Detección y análisis:** En la Fase dos la NIST (NIST, 2020) menciona la importancia de abordar adecuadamente las debilidades o vulnerabilidades de seguridad asociadas o identificadas frente al incidente de seguridad.

Uno de los puntos importantes en esta fase es identificar los diferentes vectores de ataque que pueden ser:

- Medio externos o removibles.
- Sitios WEB.
- Correo Electrónico.
- Vulnerabilidades activas.
- Pérdida o robo de Dispositivos.

Por otra parte, tenemos como identificar señales de un incidente y llegar a definir con precisión cual es la magnitud y el problema al que puede estar expuesta la organización.

Uno de los puntos más importantes en la detección y análisis, es llegar a evaluar las fuentes como logs o los indicadores de compromiso que pueden entregar señales del tipo de incidente al que está expuesto la organización.

El análisis del incidente es fundamental, ya que logra unir y validar cada uno de los puntos referenciados anteriormente por la NIST (NIST, 2020) y tener un detalle de cada escenario.

Según el análisis realizado se hace la documentación del incidente con base en lo descrito en la Guía de referencia de gestión de incidentes de la NIST, posterior a esto se hace su clasificación, con base en lo definido en el modelo y finalmente se hace la notificación del incidente, por lo canales de comunicación definidos por la organización basados en las recomendaciones entregadas por la NIST en el punto 3.2.7 de la guía (NIST, 2020).

- **Contención, erradicación y recuperación:** Como se indica por la NIST (NIST, 2020), son cuatro puntos para tener en cuenta y hacer una correcta contención erradicación y recuperación del incidente:

- Seleccionar una estrategia de contención.
- Recopilación y manejo de pruebas.
- Identificar los atacantes.
- Erradicar y recuperar los activos comprometidos.

Dando alcance a cada una de las etapas anteriormente se puede aplicar buenas prácticas de acuerdo con lo propuesto en el modelo de la NIST.

- **Actividades Post-Incidente:** En esta etapa la NIST es muy enfática en tener claro el tema de lecciones aprendidas ya que permite la mejora continua ante futuros incidentes de seguridad, en donde se logra consolidar las matrices de amenazas, vectores de ataques, comportamientos y la forma como se actúa ante su contención.

Todo lo mencionado anteriormente permite dar continuidad a los siguientes puntos que deben ser tenidos en cuenta en esta etapa como lo indica la NIST (NIST, 2020):

- Uso de Datos de incidentes pasados, bases de conocimiento.
- Retención de Evidencias.
- Lista de Verificación del manejo del incidente.

Finalmente, con base en las etapas que propone la NIST en su guía de Gestión de incidentes permite aplicar a los modelos organizacionales para adoptar las prácticas y moldear de acuerdo con la necesidad.

5.4.3. ISO 27035:2023

Otro marco de referencia frente al modelo de Gestión de incidentes es el definido por la ISO (ANSI, 2023) 27035:2023 **nombrado** “ISO/IEC 27035-1: Tecnología de la información — Técnicas de seguridad — Gestión de incidentes de seguridad de la información — Parte 1: Principios de gestión de incidentes.” a diferencia del Modelo de NIST este está compuesto por cinco etapas:

- Planificación y preparación
- Detección y reportes
- Evaluación y decisiones
- Respuesta
- Lecciones Aprendidas.

Estos modelos al igual que la ISO/IEC 27035-2: Tecnología de la información — Técnicas de seguridad — Gestión de incidentes de seguridad de la información — Parte 2: Directrices para planificar y preparar la respuesta a incidentes (ANSI, 2023). Serán tenidas en cuenta para el desarrollo de este proyecto.

5.4.4. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del MinTIC.

El modelo de gestión de incidentes de seguridad de la información propuesto por el MinTIC (MINTIC, 2016) tiene como objetivo “tener un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información”, en donde plasma varios objetivos y resaltamos los que se consideran más importantes:

- Definir roles y responsabilidades dentro de la Organización como eje puntual para evaluar los riesgos y permita mantener la operación, la continuidad y la disponibilidad del servicio. (MINTIC, 2016) El tema de Roles y

responsabilidades tomado como referencia de la NIST 800-61 con foco de riesgos.

- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información. (MINTIC, 2016) uno de los temas claves en la clasificación de incidentes para dar un buen direccionamiento al proceso.
- Consolidar las lecciones aprendidas que dejan los incidentes de seguridad de la información y su gestión para aprender rápidamente. Esto tiene como objeto incrementar las oportunidades de prevenir la ocurrencia de futuros incidentes mejorar la implementación y el uso de las salvaguardas y mejorar el esquema global de la gestión de incidentes de seguridad de la información (MINTIC, 2016). Las lecciones aprendidas son una de las fases más importantes para la documentación de incidentes y aplicar la mejora continua para próximos escenarios, donde se presente incidentes del mismo tipo.
- Definir los procedimientos formales de reporte y escalada de los incidentes de seguridad. (MINTIC, 2016) También conocido como matriz de escalamiento en todo el proceso de gestión de incidentes de seguridad.

Según lo propuesto por el MinTIC se debe tener en cuenta los siguientes procesos o etapas:

Ilustración 2 Ciclo de vida de la gestión y respuesta a un incidente de seguridad



Autor: (MINTIC, 2016)

Una de las recomendaciones entregada por el MinTIC en su documento (MINTIC, 2016) es que se establezca un equipo de respuesta a incidentes conocido como CSIRT, donde se definan todos los procesos, actividades y flujos que debe tener la gestión de un incidente de seguridad desde su identificación a su erradicación y cierre correspondiente.

A continuación, se resume cada una de las fases relacionadas en la Ilustración 2:

- **Preparación:** Se define todo lo relacionado a recursos de comunicación desde una identificación del incidente y los canales donde se debe transmitir, el hardware y software necesarios para la correcta gestión de los incidentes de los equipos participantes, los recursos necesarios para hacer un correcto análisis del incidente identificado, finalmente los recursos que son necesarios para hacer una mitigación y remediación adecuada frente al incidente de seguridad.

- **Detección y análisis:** En esta etapa se hace la detección identificación y gestión de los elementos que determinan los indicadores que aplican para un incidente de seguridad. Fase de análisis, es donde se realiza la parte de comportamientos y anomalías del evento iniciador, comparando con la base de conocimiento de la organización y diferentes fuentes de información que den indicio de lo sucedido. Posterior a esto se hace una evolución o valoración para determinar qué impacto puede generar sobre la organización. Para pasar a la fase de clasificación del incidente de seguridad, donde se tiene definido las categorías alineado a los riesgos de la organización. En la siguiente parte se realiza la fase de priorización, donde se determinan variables que permiten determinar que prioridad recibe y atención por parte de las áreas responsables para saber su tiempo de respuesta, según lo definido por la entidad u organización. Finalmente se hace la parte de declaración o notificación del incidente, con base en lo definido por la organización y aplicar lo establecido por el proceso para tomar acciones de manera oportuna en los incidentes.
- **Contención erradicación y recuperación:** En esta etapa es importante implementar estrategias que permita tomar decisiones de acuerdo con lo mencionado por el MinTIC (MINTIC, 2016), con el fin de disminuir daños y afectar la triara de seguridad (confidencialidad, integridad y disponibilidad). La entidad o u organización que adopte esta fase debe tener previamente definida sus estrategias

y Playbooks de cómo actuar ante estas situaciones y contener, erradicar y recuperarse de las posibles afectaciones bajo los casos de uso más comunes que se establezcan.

- **Actividades Post-Incidente:** Es una de las actividades más importante para la entidad ya que esta fase es la que permite dejar documentado todo el flujo de trabajo desde la identificación del incidente y las decisiones y acciones ejecutadas, ayudando a identificar oportunidades de mejora que ayuden a la mejora continua del proceso para futuros escenarios similares. Finalmente ayuda a detallar la línea de tiempo para ver comportamientos que permitan mejorar los casos de uso para ese tipo de amenazas.

Finalmente, la guía de gestión de incidentes de seguridad del MinTIC tiene como base las normas mencionadas en los puntos 6.1 y 6.2 y lo adapta de acuerdo con el modelo de gobierno para las entidades públicas.

5.4.5. CIS control V8 CSC17 - Gestión de Respuesta a Incidentes.

El CIS control es un estándar de buenas prácticas de seguridad de Center for Internet Security y está compuesto por 18 Controles críticos (CSC) en su última versión del 2022 (Center for Internet Security, 2021), entre estos controles se encuentra el CSC numero 17

nombrado “Gestión de Respuesta a Incidentes”, donde se relaciona su criticidad, procedimientos y/o herramientas y las salvaguardas que lo componen.

Ilustración 3 Salvaguardadas de Gestión de Incidentes CSC17 CIS V8

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
17.1	Designar personal para administrar el manejo de incidentes Diseñe una persona clave, y al menos una persona como respaldo, que gestionará el proceso de gestión de incidentes de la empresa. El personal de administración es responsable de la coordinación y documentación de la respuesta a incidentes y los esfuerzos de recuperación y puede consistir en empleados internos de la empresa, proveedores externos o un enfoque híbrido. Si utiliza un proveedor externo, designe al menos una persona interna de la empresa para supervisar cualquier trabajo de terceros. Revise anualmente o cuando ocurran cambios importantes en la empresa que puedan afectar esta protección.	N/A	Responder	●	●	●
17.2	Establecer y mantener información de contacto para informar incidentes de seguridad Establecer y mantener la información de contacto de las partes que necesitan ser informadas de incidentes de seguridad. Los contactos pueden incluir personal interno, proveedores externos, fuerzas del orden, proveedores de seguros cibernéticos, agencias gubernamentales relevantes, socios del Centro de Intercambio y Análisis de Información (ISAC) u otras partes interesadas. Verificar los contactos anualmente para asegurarse de que la información está actualizada.	N/A	Responder	●	●	●
17.3	Establecer y mantener un proceso empresarial para informar de incidentes Establezca y mantenga un proceso de la empresa para que la plana laboral informe de incidentes de seguridad. El proceso incluye el plazo de presentación de informes, el personal al que informar, el mecanismo de presentación de informes y la información mínima que se debe informar. Asegúrese de que el proceso esté disponible públicamente para toda la plana laboral. Revisar esta salvaguarda anualmente, o cuando se produzcan cambios significativos en la empresa que puedan afectar a esta Salvaguarda.	N/A	Responder	●	●	●
17.4	Establecer y mantener un proceso de respuesta a incidentes Establezca y mantenga un proceso de respuesta a incidentes que aborde los roles y responsabilidades, los requisitos de cumplimiento y un plan de comunicación. Revise anualmente o cuando ocurran cambios importantes en la empresa que puedan afectar esta salvaguarda.	N/A	Responder	●	●	●
17.5	Asignar Roles Claves y Responsabilidades Asigne roles claves y responsabilidades responder a incidentes, incluido el personal de legal, TI, seguridad de la información, instalaciones, relaciones públicas, recursos humanos, personal de respuesta a incidentes y analistas, según corresponda. Revise esta salvaguarda anualmente o cuando ocurran cambios importantes en la empresa que puedan afectar esta protección.	N/A	Responder	●	●	●

Autor: (Center for Internet Security, 2021)

Ilustración 4 Salvaguardadas de Gestión de Incidentes CSC17 CIS V8 parte 2

SALVAGUARDA	TÍTULO DE SALVAGUARDA/DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
17.6	Definir mecanismos de comunicación durante la respuesta a incidentes Determine qué mecanismos principales y secundarios se usarán para comunicarse e informar durante un incidente de seguridad. Los mecanismos pueden incluir llamadas telefónicas, correos electrónicos o cartas. Tenga en cuenta que ciertos mecanismos, como los correos electrónicos, pueden verse afectados durante un incidente de seguridad. Revisar anualmente, o cuando se produzcan cambios significativos en la empresa que puedan afectar a esta Salvaguarda.	N/A	Responder			
17.7	Realizar ejercicios rutinarios de respuesta a incidentes Planifique y lleve a cabo ejercicios y escenarios de respuesta a incidentes de rutina para el personal clave involucrado en el proceso de respuesta a incidentes a fin de prepararse para responder a incidentes del mundo real. Los ejercicios deben probar los canales de comunicación, la toma de decisiones y los flujos de trabajo. Realice pruebas anualmente, como mínimo.	N/A	Recuperar			
17.8	Realizar revisiones posteriores a un incidente Realice revisiones posteriores al incidente. Las revisiones posteriores al incidente ayudan a prevenir la repetición del incidente mediante la identificación de lecciones aprendidas y acciones de seguimiento.	N/A	Recuperar			
17.9	Establecer y mantener umbrales de incidentes de seguridad Establezca y mantenga umbrales de incidentes de seguridad, incluyendo, como mínimo, la diferenciación entre un incidente y un evento. Los ejemplos pueden incluir: actividad anormal, vulnerabilidad de seguridad, debilidad de seguridad, violación de datos, incidente de privacidad, etc. Revisar anualmente, o cuando se produzcan cambios significativos en la empresa que puedan afectar a esta Salvaguarda.	N/A	Recuperar			

Autor: (Center for Internet Security, 2021)

Adicionalmente en la definición de procesos el CIS indica que “aunque no se cuente con recursos para implementar un proceso de gestión de incidentes es fundamental contar con plan básico” (Center for Internet Security, 2021) que permita armar la reacción ante estos escenarios, por medio de las salvaguardas relacionadas anteriormente.

El CIS control es uno de los framework que hace match con el Framework de Ciberseguridad de la NIST en sus funciones de seguridad, donde se identifica la parte de Responder y Recuperar.

5.4.6. ISO27001:2022 – Apartado Gestión de Incidentes.

La norma ISO 27001 es reconocida en el mercado por ser uno de los modelos de referencia para definir los lineamientos de seguridad de la información y en su última versión del 2022, se exponen puntos relacionados con el tema de gestión de incidentes de seguridad de la información donde referencian lo siguiente:

Tabla 1 Controles Gestión de Incidentes ISO27001:2022

Control	Norma	Descripción
A.5.24	ISO 27001:2022	Planeamiento y preparación de la gestión de incidentes de seguridad de la información
A.5.25	ISO 27001:2022	Evaluación y decisión en los eventos de seguridad de la información
A.5.26	ISO 27001:2022	Respuesta a los incidentes de seguridad de la información
A.5.27	ISO 27001:2022	Aprendizaje sobre los incidentes de seguridad de la información
A.5.28	ISO 27001:2022	Recolección de evidencia
A.6.8	ISO 27001:2022	Reportes de eventos de seguridad de la información

Autor: Tomado del anexo A ISO27001:2022 (ISO/IEC 27001, 2022)

Por medio de los lineamientos que aporta la ISO 27001:2022 en sus controles enfocados para la gestión de incidentes de seguridad de la información, se tiene claro el

alcance de lo que se debería realizarse para dar cumplimiento a la gestión de incidentes de seguridad, aunque no profundiza mucho en este proceso es de gran valor aplicar los controles relacionados anteriormente. Para temas de profundización e implementación nos podemos remitir a la guía de implementación de la ISO 27002:2022.

5.4.7. Comparación de marcos de Referencia.

Tabla 2 Comparación marcos de referencia

Aspecto	CIS V8 CSC17	NIST 800-61 Rev. 2	ISO 27035:2023	Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del MinTIC	ISO27001:2022 – Apartado Gestión de Incidentes
Alcance	Está Enfocado en aplicar buenas prácticas al proceso de gestión de incidentes.	Está enfocado en la seguridad Cibernética.	Está enfocada en Seguridad de la Información.	Está enfocada en entidades públicas alineado a la NIST y 27035.	Está enfocada en sistema de gestión de seguridad de la información.
Objetivo	Establecer un programa para desarrollar y mantener una capacidad de respuesta a incidentes.	Preparación y definición de fases para la respuesta a incidentes.	Permite orientar como establecer e implementar el proceso para la gestión de incidentes de seguridad de la información.	Ofrecer guía para la gestión de incidentes basado en las buenas prácticas para entidades públicas.	Da definiciones de lo que debe tener un proceso para gestionar incidentes de seguridad

Proceso de Gestión de Incidentes	No define etapas, pero define los requisitos que se deben tener en cuenta en la práctica de la gestión de incidentes.	Define las etapas que debe tener la gestión de incidentes: Preparación, Detección, Análisis, Contención, Erradicación, Recuperación y Lecciones Aprendidas	Define las etapas que debe tener la gestión de incidente: preparación, detección y reportes, análisis y evaluación, respuesta y contención, recuperación y restauración, lecciones aprendidas.	Define las etapas que debe tener la gestión de incidentes: detección, análisis, contención, erradicación, recuperación y lecciones aprendidas	Define las etapas que debe tener la gestión de incidentes: Identificación, registro, evaluación, respuesta y seguimiento
Roles y responsabilidades	Definidos por la organización de acuerdo con las recomendaciones.	Definidos por la organización de acuerdo con las recomendaciones.	Definidos por la organización de acuerdo con las recomendaciones.	Definidos por la organización de acuerdo con las recomendaciones y ámbito público.	Definidos por la organización de acuerdo con las recomendaciones.
Comunicación	Interna/Externa	Interna/ Externa	Interna/ Externa	Interna/ Externa	Interna/ Externa
Gestión de riesgos	No está especificado.	Se centra más en el proceso de gestión de Incidentes.	Considera el riesgo en todo el proceso de gestión de incidentes.	Se menciona en el análisis e impacto del riesgo.	Se considera la evaluación de riesgo basado en probabilidad e impacto.

Mejores prácticas y controles	Listados de controles específicos para aplicar a procesos ya definidos.	Guías y mejores prácticas recomendadas	Proporciona orientación sobre mejores prácticas y controles específicos para la gestión de incidentes de seguridad de la información.	Controles y mejores prácticas sugeridas en las normas de la NIST y 27035.	Listados de controles específicos basado en el proceso.
Enfoque tecnológico	Herramientas de seguridad y buenas prácticas.	Herramientas y tecnologías adecuadas.	Herramientas y tecnologías para la gestión de incidentes de seguridad.	Herramientas y tecnologías adecuadas.	Definido más al proceso no tiene enfoque tecnológico.
Evaluación y mejora continua	Revisión y mejora de los controles	Evaluación constante y la mejora continua.	Parte integral del proceso de gestión de incidentes para garantizar la eficacia y eficiencia continua	Se enfoca en la mejora continua del proceso definido por cada entidad que lo aplique.	Integral en el sistema de gestión de seguridad de la información.

Autoría: Tomado de cada uno de los modelos mencionados. (Center for Internet Security, 2021), (NIST, 2020), (ANSI, 2023), (MINTIC, 2016) y (ISO/IEC 27001, 2022).

6. MARCOS DE REFERENCIA

6.1.¿QUIÉN ES EL ITFIP?

El Instituto Tolimense de Formación Técnica Profesional ITFIP fue creado mediante el Decreto No. 3462 de diciembre 24 de 1.980 expedido por el Ministerio de Educación Nacional.

En cumplimiento de la Ley 24 de 1.988 se organiza como un establecimiento público del orden nacional denominado: Instituto Tolimense de Formación Técnica Profesional “ITFIP” adscrito al Ministerio de Educación Nacional como Establecimiento de Educación Superior de carácter Técnico Profesional.²

Los Objetivos del ITFIP son:

Incrementar la cobertura académica a través de la ampliación de la oferta de programas académicos pertinentes, currículos dinámicos y mejoramiento de las competencias de docentes con el fin de fortalecer la autoevaluación como proceso inherente a la acreditación institucional y aseguramiento de la calidad.

Consolidar el proceso de investigación en docentes y estudiantes a través de estrategias que permitan la creación, difusión y aplicación de conocimiento en las

² *ITFIP* | *ITFIP*, <https://itfip.edu.co/>.

diferentes áreas del saber; con el objeto de aplicar los resultados en la dinámica académica, regional y diferentes grupos de interés gubernamental y privado.

Ampliar la proyección nacional e internacional del ITFIP mediante el establecimiento de alianzas y desarrollo de estrategias de interacción, con el fin de promover convenios con otras universidades y organismos internacionales que faciliten el financiamiento de proyectos o programas de formación, pasantías y movilidad para la comunidad académica.

Mejorar la calidad de vida y generar un ambiente óptimo de bienestar para estudiantes, egresados, funcionarios docentes y administrativos con el fin de fortalecer el sentido de pertenencia y la formación integral dentro del marco de los principios y valores institucionales.

Fortalecer el proceso de mejoramiento de la gestión institucional e interacción de procesos, con el fin de mantener la eficacia, eficiencia y efectividad en las actuaciones internas y externas de la institución.

6.1.1. Misión del ITFIP

“El Instituto Tolimense de Formación Técnica Profesional – ITFIP, formar profesionales íntegros, líderes transformadores del entorno Regional y Nacional con criterio global, tecnológico, ambiental para el desarrollo social, económico y cultural en el marco de la convivencia y la paz”.

6.1.2. Visión del ITFIP

“En el 2024, el Instituto Tolimense de Formación Técnica Profesional – ITFIP, será reconocido por sus programas académicos de alta calidad y el liderazgo en la formación de profesionales íntegros, emprendedores, gestores de un proyecto de vida que transforme su entorno y contribuya al desarrollo ambiental y sostenible de la región y la Nación, en un contexto globalizado, fortaleciendo la cultura de la paz.”

6.1.3. Servicios del ITFIP

Los servicios que ofrece el ITFIP son por medio de los Registros Calificados para los programas profesionales universitarios en Administración de Empresas, Administración Agropecuaria y Contaduría Pública en el 2008 y en el 2012 se obtuvo los Registros Calificados para ofertar Ingeniería Electrónica, Ingeniería Civil e Ingeniería de sistemas (por ciclos propedéuticos).

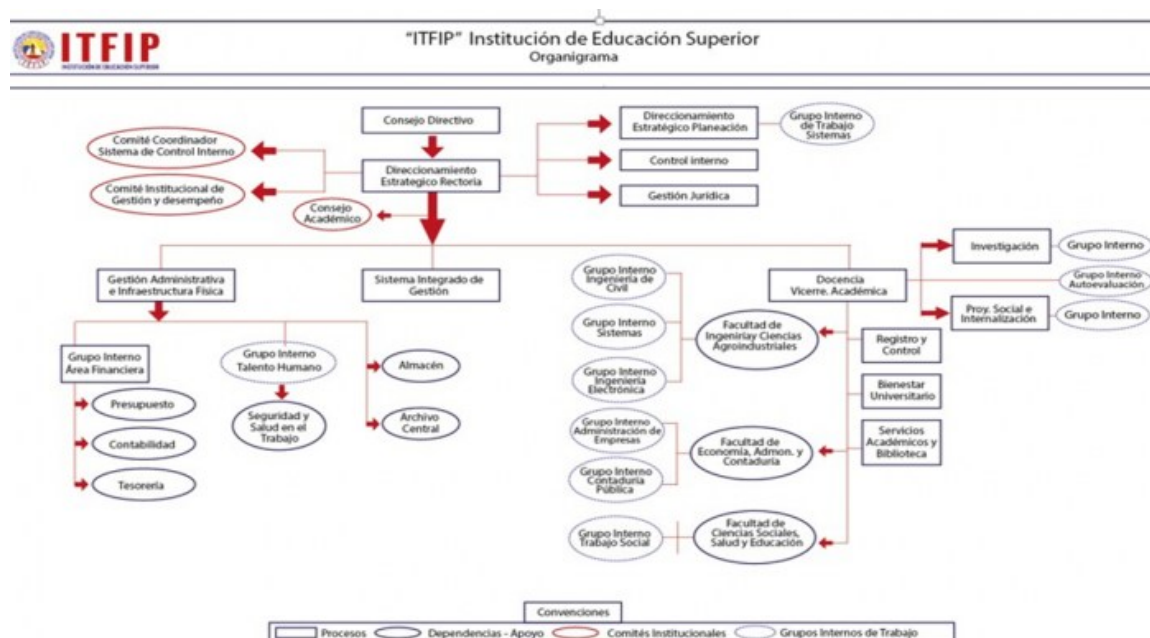
Al ser institución educativa con gran experiencia en el sector educativo permite ofertar programas de educación superior en los diferentes campos a estudiantes de la región, bajo la supervisión del Ministerio de Educación.

Además, cuenta con equipo de docentes altamente calificados para brindar los servicios educativos ofertados y con equipo administrativo y tecnológico por detrás que permite brindar soporte y apoyo a todos los estudiantes del ITFIP.

6.1.4. Organigrama del ITFIP

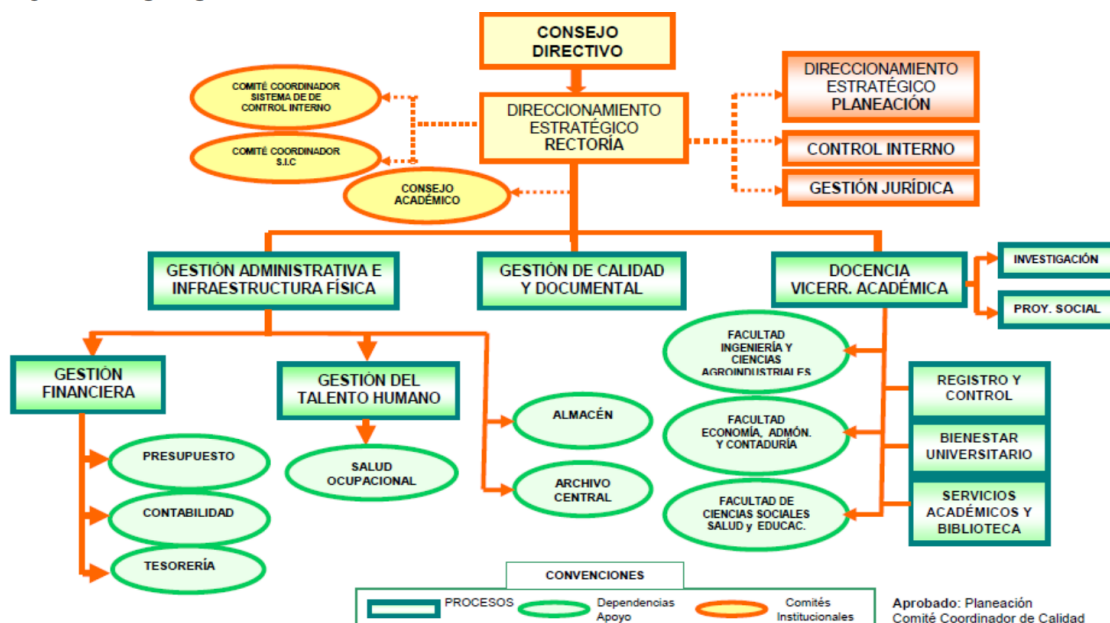
En la Ilustración 5, se identifica el organigrama de la Institución educativa ITFIP:

Ilustración 5 Organigrama ITFIP



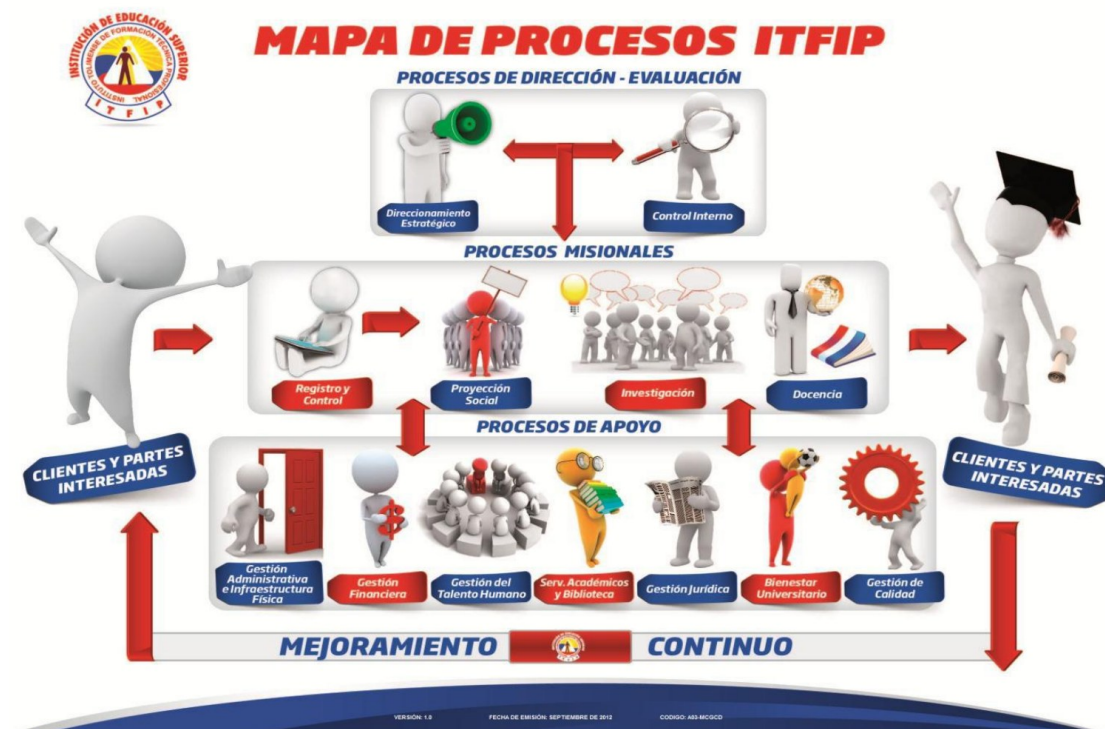
Fuente: Información Suministrada por ITFIP del Sistema de gestión de Calidad.

Ilustración 6 Organigrama Directivo ITFIP



Fuente: Información Suministrada por ITFIP del Sistema de gestión de Calidad.

Ilustración 7 Mapa de Procesos ITFIP



Autor: Información Suministrada por ITFIP del Sistema de gestión de Calidad.

Se identifica que la Universidad ITFIP no cuenta con un proceso de gestión de incidentes de ciberseguridad, y se debe plantear la definición e inclusión de este en el Proceso de Apoyo.

7. Marco Legal

La universidad ITFIP al ser una institución educativa de educación superior debe acogerse a las normativas y leyes de la función pública y las establecidas por MEN (Ministerio de Educación Nacional), adicionalmente como todas las entidades debe cumplir con todo lo relacionado al tratamiento de datos personales de manera obligatoria.

Teniendo en cuenta las normativas y leyes asociadas a ciberseguridad se deben tener en cuenta las siguientes relacionadas en la tabla 3 del Normograma:

Tabla 3 Normativas

ítem	Norma	Descripción
1	Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. ³
2	Conpes 3701 del 14 de julio de 2011.	Lineamientos de política para Ciberseguridad y Ciberdefensa. ⁴

³ (Reservado, 2023)

⁴ (Ministerio de Educación)

3	Política de Seguridad Digital MinTIC	Se basa en unos principios fundamentales, que contemplan: Salvaguardar los derechos humanos y los valores fundamentales de los individuos. Adoptar un enfoque incluyente y colaborativo que involucre activamente a todos los interesados. (“Política de Seguridad Digital - MINTIC Colombia”) Asegurar una responsabilidad compartida entre todos los actores involucrados. ⁵
4	Ley 1266 2008	"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones." (“DECRETO 2952 DE 2010 - SUIN – JURISCOL”) ⁶
5	Ley 1273 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"-y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. ⁷

⁵ (Ministerio de Educación)

⁶ (Reservado, 2023)

⁷ (Reservado, 2023)

6	Ley 1581 2012	"Por la cual se dictan disposiciones generales para la protección de datos personales." ("Consulta de la Norma - OAS")
7	Ley 1712 2014	"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones." ("LEY 1712 DE 2014 - SUIN – JURISCOL")
8	Conpes 3854 2016	Política Nacional de Seguridad Digital.
9	Decreto 2693 2012	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
10	Decreto 1377 2013	"Por el cual se reglamenta parcialmente la Ley 1581 de 2012." ("DECRETO 1377 DE 2013 - SUIN – JURISCOL")

Autor: Propio consolidado.

Adicionalmente, se debe tener en cuenta las siguientes normas que son aplicables al ITFIP, por ser Institución de educación del sector público en ámbitos de Seguridad en datos y Ciberseguridad:

- **Decreto 1008 de 2018:** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro

2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".⁸

- **Conpes 3701 de 201:** Busca generar lineamientos de política en ciberseguridad y ciberdefensa, orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.⁹
- **"Conpes 3920 de 2018:** Política Nacional de Explotación de Datos." ("Leyes, Decretos y Normas para la Transformación Digital")¹⁰
- **Conpes 3670 de 2010:** Lineamientos de política para la continuidad de los programas de acceso y servicio universal a las tecnologías de la información y las comunicaciones.¹¹

⁸ (Reservado, 2018)

⁹ (Reservado, s.f.)

¹⁰ (Reservado, 2018)

¹¹ (Reservado, 2010)

8. MARCO TECNOLÓGICO

Para lograr este desarrollo del marco tecnológico, la gestión de incidentes de ciberseguridad involucra un modelo definido con los procesos de manera cíclica como hace referencia la norma NIST-800-61 Computer Security Incident Handling Guide (<http://www.nist.gov>) (NIST, 2020).

Las etapas del procedimiento de la gestión de incidentes de ciberseguridad, según (MINTIC, 2016) incluyen las siguientes:

- Planificación y preparación para la gestión de incidentes.
- Detección y análisis.
- Contención, erradicación y recuperación.
- Actividades, Post-incidente.

Estos procesos incorporan una serie de actividades que van alineados con la NIST (NIST, 2020) y acompañados de la normativa ISO-IEC 27035-2023 (ANSI, 2023) para el mejoramiento desde la gestión de gobierno hacia los demás procesos y controles de ciberseguridad.

El instituto (ITFIP) en su infraestructura que cuenta con tecnología de marca Fortinet en su mayoría, en condiciones óptimas a nivel operativa y de capacidad, la cual está compuesta por los siguientes componentes de seguridad:

- Dos (2) FortiGate 1500 D

Esta solución hace parte de los dispositivos de seguridad perimetral de próxima generación NGFW con un alto desempeño, este dispositivo permite la

interacción de tráfico norte-surte, mediante el aseguramiento de enrutamiento del origen y destino por medio de políticas, protocolos, servicios, listas blancas y demás objetos en la red. (Fortinet, 2021)

- Un (1) FortiADC 400F

Este dispositivo actúa como controlador de aplicaciones corporativa, garantizando que esta misma aplique la disponibilidad, seguridad y optimización en aplicaciones, cuenta con características que actúa como WAF para protección de aplicaciones web, protección DDOS para el control de denegación de servicios y AV como actuador frente a amenazas de malware. (Fortinet, 2023)

- Un (1) FortiAnalyzer-300G

Actuador analítico sobre amenazas avanzadas en los procesos de orquestación, automatización y respuesta, con el fin de reducir riesgos mejorando la seguridad interna y externa de la organización y cuenta con módulo de reportes. (Fortinet, 2023)

- Un (1) FortiWeb-400E

Es un tipo de control de la capa de aplicación en los sitios web, protegiendo la seguridad expuesta de las páginas web y API contra ataques dirigidos, modela este tipo de ataques, aplicando la contención y defiende sobre vulnerabilidades del sistemas y amenazas de día cero. (Fortinet, 2023)

- Un (1) FortiSandbox FSA-500F

Dispositivo dedicado a la solución de protección de amenazas avanzadas (ATP), a través de la detección y mitigación de amenazas de malware, su procesamiento basado en modelos y casos de uso para la inteligencia procesable en tiempo real. (Fortinet, 2023)

- Un (1) FortiSIEM FSM-2000F

Es un centralizador de información de diferentes fuentes de red y sistemas Core de negocio, que permite la recopilación de los datos y análisis de diferentes fuentes de información; de esta manera mediante modelos, casos de uso se generan alertas que permiten tomar decisiones respecto a las interacciones y anomalías que suceden en la red. (Fortinet, 2023)

- Ocho (8) FortiAPs FAP-U431F-N

Permite la administración los puntos de acceso hacia la red corporativa, para el monitoreo y gestión sobre la red de forma segura y administrable; contiene un punto de acceso de tipo portal de gestión integrado al controlador de WLAN. (Fortinet, 2023)

- Ocho (8) FortiSwitch FS-124F-POE

FortiSwitch permite la administración controlada de los accesos a la red con un panel de administración con el enfoque de visibilidad en el control de acceso de los servicios y los usuarios. (Fortinet, 2023)

De acuerdo con las herramientas mencionadas anteriormente, se puede llegar a contener los agentes de amenazas que materializan los incidentes de seguridad, a nivel general pueden existir cualquier cantidad de herramientas, pero pueden llegar a clasificarse de la siguiente manera:

- Herramientas Físicas: Appliances y servidores.
- Herramientas de Software: Scripts, analizadores de tráfico, SIEM (fortisiem), datalakes, entre otros.
- Herramientas Distribuidas: Kali Linux y kits forenses.

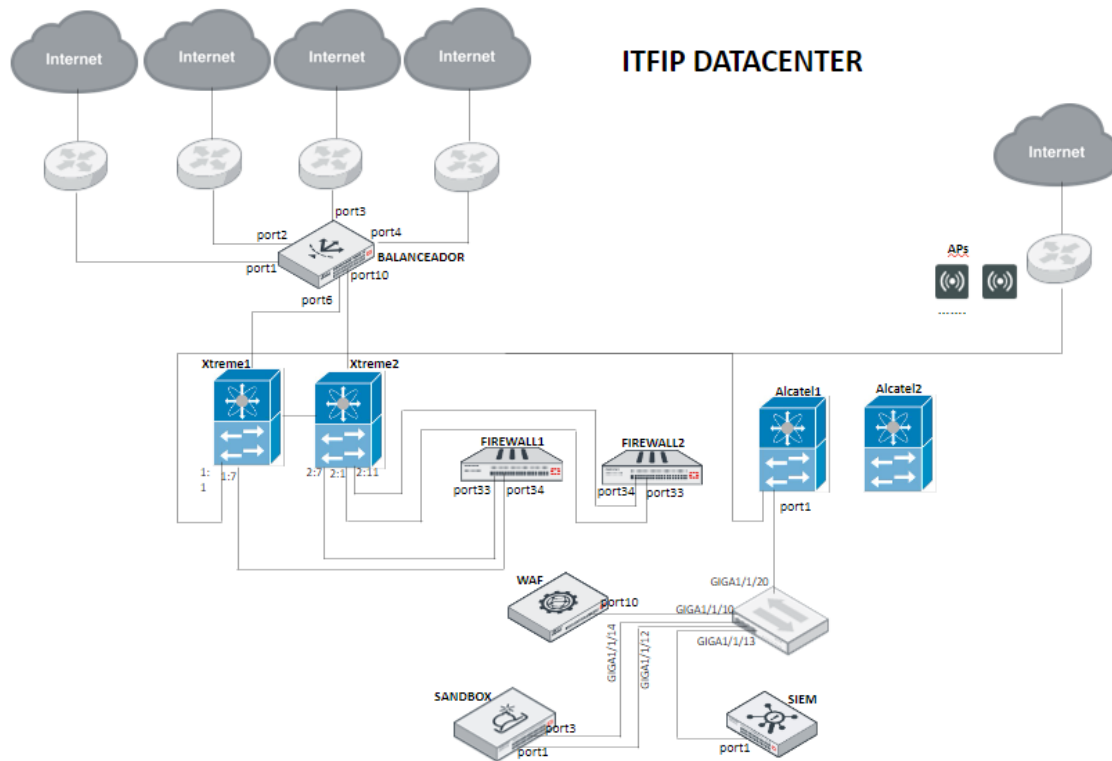
- Agentes Autónomos o independientes controlados de manera centralizada.
- Documentales: Bitácoras, playbooks, instructivos y matrices.

En el ámbito tecnológico es importante conocer los agentes de amenazas, para generar su clasificación y una de las herramientas o frameworks que permiten apoyar en este proceso de identificar los vectores de ataque. El MITRE denominado ATT&CK el cual cuenta con las tácticas y técnicas basados en las observaciones del mundo real, además de contar con una base de conocimiento ATT&CK la cual esta desarrollada por modelos y metodologías de amenazas en todos los ámbitos y sectores (MITRE, 2023).

El ITFIP en toda su infraestructura tecnológica cuenta con herramientas que son claves en toda la definición de los procesos de gestión de incidentes y que permiten a los administradores tener aseguramiento de los datos y la información, el objetivo es que toda esta tecnología permita apalancar el proceso para saber cómo utilizarlas y actuar ante una situación de riesgo cibernético que comprometa la Universidad y definir una buena toma de decisiones ante un incidente de seguridad.

A continuación, se detalla el diagrama de arquitectura con la infraestructura adoptada por el ITFIP:

Ilustración 8 Arquitectura de Referencia



Autor: ITFIP

Por medio del grafico anterior se logra tener un esquema de cómo está la infraestructura.

9. DISEÑO METODOLÓGICO

De acuerdo a lo definido por (Hernández Sampieri, Fernández Collado, & Batista Lucio, 2014) menciona que enfoque de investigación cualitativo es “Utilizar la recolección y análisis de los datos para afinar preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación”¹² y el enfoque de investigación cuantitativo es “Utiliza la recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico, con el fin de establecer pautas de comportamiento y probar teorías”¹³.

- **Tipo de Investigación:** Con base en los dos modelos de investigación descritos anteriormente, el enfoque de esta investigación es de tipo mixto ya que se tendrá en cuenta orientaciones cuantitativas y cualitativas que permitirán ejecutar el proceso investigativo de una manera general, donde se desarrollaron entrevistas, definiciones, conceptos, opiniones, oportunidades de mejora hasta llegar a lo específico que permite tener resultados basados en métricas, indicadores (KPI o KRI) de referencia para toma de decisiones e identificar comportamientos.

Este tipo de investigación permite entender mejor la problemática identificada en el ITFIP en el proceso de Gestión de Incidentes de Ciberseguridad, para abordar en cada uno de los escenarios; permitiendo analizar y definir las mejores prácticas para este proceso.

¹² (Hernández Sampieri, Fernández Collado, & Batista Lucio, 2014)

¹³ (Hernández Sampieri, Fernández Collado, & Batista Lucio, 2014)

- **Fuentes de Investigación:** La información que se usara en el desarrollo del proyecto es fundamental, ya que se trabajara con lo suministrado por la entidad ITFIP, donde se recibirá información verbal, digital y descriptiva por parte de los colaboradores que hacen parte del proceso de Tecnología, contratistas y terceros involucrados.
- **Recolección y análisis de información:** Se recolecta la información por medio de sesiones de trabajo, visitas y entrevistas con los colaboradores del ITFIP, documentación publica de la página web, interna, organizándola en varias herramientas ofimáticas, para las justificaciones requeridas en el proyecto.
- **Acciones:** Cada objetivo específico será trabajado como una etapa del proyecto, permitiendo ejecutar diferentes actividades que permitirán recopilar información para concluir los resultados obtenidos.

A continuación, se describen cada una de las etapas que se desarrollaran con base en los objetivos específicos como se muestra en la tabla 4:

Tabla 4 Marco Metodológico

Objetivos Específicos	Diseño Metodológico
Identificar si existen subprocesos de seguridad o ciberseguridad en el mapa de procesos del ITFIP en la parte tecnológica, permitiendo	Por medio de una investigación cualitativa se desarrollarían las siguientes actividades: • Solicitar y analizar el Mapa de procesos del ITFIP.

establecer cómo se incluirá el proceso de gestión de incidentes de seguridad y ciberseguridad; generando un GAP (Análisis de brecha), para determinar que se debe tener en cuenta para la inclusión del nuevo proceso.

- Identificar donde se incluirá el proceso de gestión de incidentes de seguridad y ciberseguridad de acuerdo con el análisis realizado.

- Generar el GAP (Análisis de brecha) con las acciones a tomar para inclusión del proceso de gestión de incidentes y las actividades administrativas que se deben realizar con el ITFIP.

Diseñar y proponer un proceso de gestión de incidentes de seguridad y ciberseguridad para el ITFIP mediante los modelos y framework de buenas prácticas que propone la ISO 27035:2023, la NIST 800-61 Rev-2 y la Guía de Gestión de Incidentes del MinTIC, para estructurar el proceso, guías y

Por medio de una investigación mixta permite desarrollar las siguientes actividades:

- Documentarse sobre los framework ISO27035:2022, NIST 800-61 Rev-2 y la Guía de Gestión de incidentes de seguridad del MINTIC.
- Generar entrevistas con las áreas que deberían estar a cargo del proceso de gestión de incidentes.

definiciones de la gestión de incidentes.

- Verificar si se cuenta con la política o lineamientos asociados a la gestión de incidentes y actualizar o acompañar en su definición.

- Proponer las etapas que van a ser tenidas en cuenta en el proceso de gestión de incidentes.

- Proponer los roles y responsabilidades y personal necesario por la atención de los incidentes de seguridad y Ciberseguridad.

- Proponer la matriz de escalamiento interna y externa.

- Proponer los documentos que deben apoyar el proceso de gestión de incidentes.

- Proponer de métricas e indicadores de referencia, para la mejora continua.

- Presentar diseño y propuesta a los directivos y responsables del proceso de gestión de incidentes del ITFIP.

Implementar el proceso de gestión de incidentes de seguridad y ciberseguridad con todo el flujo de trabajo, instructivos, formatos, anexos guías y definiciones de acuerdo con el diseño que adopte el ITFIP para que el equipo de tecnología pueda actuar correctamente ante un incidente de seguridad cibernético.

Por medio de una investigación mixta permite desarrollar las siguientes actividades:

- Iniciar con la fase de implementación presentada al ITFIP.
- Definir formalmente las etapas que harán parte del proceso de gestión de incidentes de ciberseguridad.
- Formalizar la matriz de roles y responsabilidades del proceso de gestión de incidentes de ciberseguridad.
- Formalizar e implementar la matriz de escalamiento interna y externa que fueron definidas para el proceso de gestión de incidentes de ciberseguridad, para su publicación.

- Formalizar e implementar los documentos propuestos para apoyar el proceso de gestión de incidentes de ciberseguridad, incluyéndolos en el sistema de calidad para su seguimiento.
- Implementar y formalizar el reporte de métricas definidas para medir el proceso de gestión de ciberseguridad, con los responsables de su medición y reporte.
- Generar acta de cierre de implementación del proceso de gestión de incidentes de ciberseguridad para su publicación y cumplimiento.

Capacitar el personal sugerido y el propuesto por los directivos del ITFIP en todas las fases del proceso de la gestión de incidentes

Por medio de una investigación mixta permite desarrollar las siguientes actividades:

- Crear un plan de concienciación sobre todo lo relacionado al proceso de

de seguridad y ciberseguridad, por medio de un plan de concientización que permita a toda la institución educativa saber cómo actuar a quien reportar y que acciones tomar ante los diferentes escenarios de un incidente de seguridad.

gestión de incidentes de seguridad y Ciberseguridad.

- Crear campañas de concienciación para todo el alumnado, personal administrativo y docente del ITFIP sobre como reportar y actuar ante un incidente de ciberseguridad.
- Dar recomendaciones y sugerencias sobre la importancia de la seguridad y ciberseguridad a nivel institucional

Generar un análisis de resultados con base en la efectividad de implementar el modelo propuesto para la gestión de incidentes de ciberseguridad del ITFIP

Por medio de una investigación mixta permite desarrollar las siguientes actividades:

- Conclusión de resultados del antes y después del proceso de gestión de incidentes de Ciberseguridad.

Autor: propio

- **Procedimiento o desarrollo metodológico:** Con base en la información presentada, se da continuidad al desarrollo de cada una de las etapas que conforman el proyecto.

9.1. ESTADO ACTUAL DE LA ENTIDAD ITFIP FRENTE AL PROCESO DE GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD CON BASE EN LAS NORAMAS TECNICAS DEFINIDAS

Actualmente la institución educativa ITFIP, no cuenta con un proceso de Gestión de Incidentes de Ciberseguridad definido, que permita atender los incidentes de ciberseguridad que puedan presentarse en su infraestructura tecnológica, plataformas y demás servicios. Es por esta razón que se vio la necesidad de apoyar a la entidad y acompañarla en el proceso, para esto se realiza una evaluación previa con base en diferentes normativas de buenas prácticas que fueron comparadas en el punto 5.4.7 (Comparación marcos de referencia), de esta tabla se consultaron los diferentes controles de cada uno de los marcos y se construyó una matriz relacionada en el ANEXO A que nos permitió evaluar los puntos clave de un proceso de gestión de incidentes de Ciberseguridad.

La herramienta que sirvió para desarrollar la evaluación y la consolidación de las buenas prácticas fue definida por los dominios más relevantes de los marcos de referencia mencionados en el punto 5, en un documento que nos permitió definir un estado actual de la entidad, adicional a esto se tuvo en cuenta recopilación y verificación de la información entregada por los funcionarios, proveedores de TI. Se realizó revisión del marco de procesos de la institución frente a como está conformada, y un análisis de su estructura organizacional.

Se desarrollaron varias entrevistas, reuniones y mesas de trabajo conjuntas con contratistas, funcionarios y proveedores de manera frecuente esporádica de acuerdo con la necesidad del proyecto. Estas fueron desarrolladas de acuerdo con lo planteado en el proyecto y alineado con la institución para ir revisando el estado y progreso de las actividades, las áreas que hicieron parte de este proceso fueron:

- Gestión de Calidad Documental.

- Tecnología.
- Gestión Administrativa.
- Vicerrectoría.

En la tabla 5 se describen las diferentes actividades y conclusiones definidas a lo largo del proyecto:

Tabla 5 Actividades del Proyecto

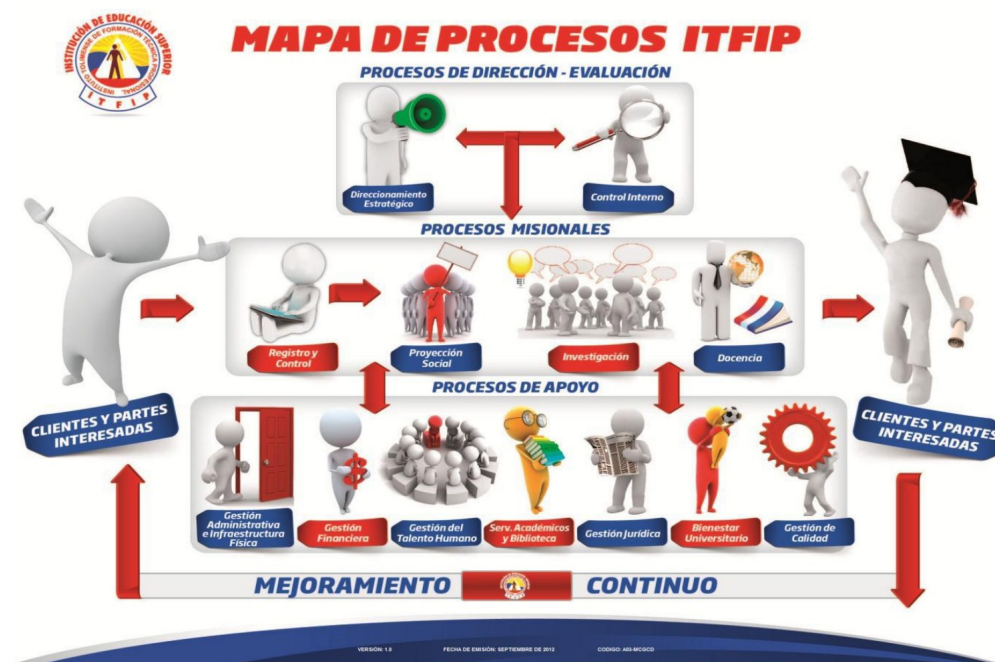
Actividades	Participantes	Mesas de Trabajo	Conclusiones
Presentación del Proyecto	Vicerrectoría, Tecnología, Gestión Administrativa	2	Después de tener conversaciones con los colaboradores del ITFIP conocer su necesidad se lleva a cabo la presentación de la iniciativa del proyecto para su aprobación por parte de la institución.
Estado actual frente al proceso de Gestión de incidentes de Ciberseguridad	Tecnología, Vicerrectoría	3	Después de varias sesiones en Teams y Meet con los diferentes colaboradores con base en el GAP definido por nosotros, consolidando las buenas prácticas de CIS V8(CSC17), NIST 800-61 Rev2, ISO 27035:2023, Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del MinTIC y la ISO27001:2022 – Apartado Gestión de Incidentes, por cada uno de los dominios se define un estado actual, donde su resultado es de solo un 3%. Claramente porque no se tenía nada frente a este proceso.
Presentación Propuesta	Vicerrectoría, Tecnología, Gestión Administrativa	1	Se da el VoBo para trabajar en lo definido a nivel documental, para la implementación y

Autor: Propio

9.1.1. Análisis mapa de procesos del ITFIP

En el mapa de procesos de la entidad se identifica que el proceso de Tecnología no está presente como se evidencia en la Ilustración 9:

Ilustración 9 Mapa de Procesos



Autor: ITFIP

De acuerdo con la justificación entregada por los colaboradores no es un proceso critico de negoció cuando se estructuro, por lo tanto, nació dentro de “Gestión Administrativa e infraestructura Física”, donde se tiene incluido la gestión de herramientas de TI y ciberseguridad, desde esta parte se logra identificar varias opciones de mejora ya que, al no tener estructura ni un proceso de Ciberseguridad, se tiene claro por donde se debe empezar a trabajar. Claramente se identifica como un proceso de Apoyo que hace parte del mejoramiento continuo.

- 9.1.2. Identificar donde se incluirá el proceso de gestión de incidentes de ciberseguridad de acuerdo con el análisis realizado.

No fue posible definirlo por parte de la institución y se definió por parte de ellos trabajar en el proceso, pero no afectar el mapa de procesos actual.

9.1.3. GAP (Análisis de brecha)

Este análisis de brecha inicia, con identificar el estado actual de la institución frente a un proceso de gestión de incidentes de Ciberseguridad, donde por medio de entrevistas, cuestionarios y reuniones se realizó una recolección de información.

9.1.3.1. Metodología:

A continuación, se relaciona los dominios que fueron tenidos en cuenta para identificar el estado actual, como se muestra en la tabla 6:

Tabla 6 Dominios Evaluados en el GAP

Ítem	Dominios
1	Alta dirección
2	Presentación de informes / indicadores
3	Procedimiento de gestión de incidentes
4	Políticas
5	Requisitos de formación, educación y sensibilización
6	Procedimientos y manuales de respuesta en el manejo de incidentes
7	Comunicación interna y externa

8	Evaluación y mejora continua
9	Roles y responsabilidades

Autor: propio consolidado de las normas (ANSI, 2023) (Center for Internet Security, 2021) (ISO/IEC 27001, 2022) (MinTIC, 2021) (NIST, 2020)

Estos fueron tomados de cada una de las normas y marcos de buenas prácticas CIS V8(CSC17), NIST 800-61 Rev2, ISO 27035:2023, Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del MinTIC y la ISO27001:2022 – Apartado Gestión de Incidentes y sus puntos en común para su construcción, los cuales fueron argumentados en el [Marco Teórico](#).

Una vez se realizó la definición de los dominios, se procedió a incorporar los 40 puntos compuestos de controles, políticas y/o lineamientos que eran pertinentes para su cumplimiento, de cada uno de los marcos, en la tabla 7 se detallan las preguntas asociadas a los controles aplicados:

Tabla 7 Preguntas del GAP

Ítem	Norma / Marco de Ref.	Descripción
1	ALTA DIRECCIÓN	
1,1	27001:2022	¿Existe un comité de seguridad y ciberseguridad con la alta dirección / comité académico? (Para la toma de decisiones)

1,2	27001:2022	¿Existen directrices o procedimientos generales para la gestión de incidentes de seguridad de la información y ciberseguridad en el ITFIP?
2	PRESENTACIÓN DE INFORMES / INDICADORES	
2,2	27001:2022	¿Existe un indicador para el reporte de incidentes de seguridad y ciberseguridad?
2,3	27001:2022	¿Existen informes periódicos que permita identificar la cantidad de incidentes y eventos reportados?
3	PROCEDIMIENTO DE GESTION DE INICIDENTES	
3,1	ISO 27001:2022	¿Se cuenta con un planeamiento y preparación de la gestión de incidentes de seguridad de la información?
3,2	NIST	¿Existe un proceso formalizado para la detección, análisis, contención, erradicación y recuperación de incidentes de seguridad de la información?
3,3	NIST/27035:2022/MinTIC	¿La institución cuenta con procedimientos documentados para la notificación y comunicación de incidentes dentro y fuera de la institución?
3,4	27035:2022/MinTIC	¿La Institución cuenta con procedimientos documentados para la detección, análisis, contención, erradicación, recuperación y lecciones aprendidas de los incidentes?
3,5	27035:2023/ CIS V8 /MinTIC	¿La Institución tiene un proceso formalizado para la gestión de incidentes de seguridad de la información?
4	POLÍTICAS	

4,1	ISO 27001:2022	¿Se cuenta con una Política de seguridad de la información y Ciberseguridad?
4,2	ISO 27001:2022	¿Se cuenta con una política general para la gestión de incidentes de seguridad y Ciberseguridad?
5	REQUISITOS DE FORMACIÓN, EDUCACIÓN Y SENSIBILIZACIÓN	
5,1	ISO 27001:2022	¿Se cuenta con Capacitaciones para el aprendizaje sobre los incidentes de seguridad y Ciberseguridad?
5,2	MinTIC	¿Se llevan a cabo actividades de sensibilización y capacitación del personal sobre la gestión de incidentes según lo sugerido en la Guía del MinTIC?
5,3	Propio	¿Hay un procedimiento de aprendizaje, teniendo en cuenta los incidentes de seguridad de la información y Ciberseguridad?
5,4	Propio	¿Se generan campañas de seguridad por mails, wallpapers, comunicados etc, sobre como reportar un incidente de seguridad?
6	PROCEDIMIENTOS Y MANUALES DE RESPUESTA EN EL MANEJO DE INCIDENTES	
6,1	ISO 27001:2022	¿ Se cuenta con un procedimiento de respuesta a los incidentes de seguridad y ciberseguridad?
6,2	ISO 27001:2022	¿Se tiene definido un procedimiento para la recolección de evidencia?
6,3	NIST	¿Se mantiene un registro de incidentes históricos y se utilizan para informar sobre las tendencias y patrones de ataques?
6,4	27035:2023	¿Se realizan evaluaciones regulares de riesgos para identificar posibles amenazas y vulnerabilidades que puedan dar lugar a incidentes de seguridad de la información?

6,5	27035:2024	¿La Institución tiene protocolos establecidos para la recopilación y preservación de evidencia forense durante la investigación de incidentes?
7	COMUNICACIÓN INTERNA Y EXTERNA	
7,1	CIS V8	¿Se tiene establecido un proceso institucional para informar un incidente?
7,2	ISO 27001:2022	¿Se tiene definido el reporte de eventos de seguridad y ciberseguridad?
7,3	27035:2023	¿Se ha establecido un proceso claro de comunicación interna y externa durante la gestión de incidentes? (Matriz de escalamiento)
7,4	MinTIC	¿La Institución cuenta con mecanismos de reporte y notificación de incidentes establecidos, en línea con las recomendaciones de la Guía del MinTIC?
7,5	MinTIC	¿Se han definido protocolos de comunicación interna y externa durante la gestión de incidentes, siguiendo las pautas proporcionadas por el MinTIC?
7,6	CIS V8	Definir mecanismos de comunicación durante la respuesta a incidentes
8	EVALUACIÓN Y MEJORA CONTINUA	
8,1	ISO 27001:2022	¿Se hace evaluación para toma de decisión en los eventos de seguridad de la información?
8,2	27035:2023/ NIST / CISV8	¿Se llevan a cabo ejercicios de simulación y pruebas para evaluar la efectividad del proceso de gestión de incidentes?
8,3	NIST 27035:2027	¿La Institución tiene un plan de mejora continua para fortalecer su capacidad de gestión de incidentes según los requisitos de la NIST 800-61 Rev. 2 /ISO 27035:2023?
8,4	27035:2026 Min TIC	¿Se documentan adecuadamente todos los incidentes, acciones tomadas y lecciones aprendidas para su análisis posterior y mejora continua?

8,5	27035:2023/ Min TIC/27001:2022	¿Existe un compromiso continuo de mejora basado en las recomendaciones y buenas prácticas proporcionadas por marcos de referencia en Gestión de Incidentes?
8,6	CIS V8	¿Se realizan revisiones posteriores a un incidente?
8,7	CIS V8	¿Se establecen y mantienen umbrales de incidentes de seguridad?
9	ROLES Y RESPONSABILIDADES	
9,1	NIST 27035:2023	¿La Institución tiene un equipo de respuesta a incidentes (IRT) designado y capacitado para manejar los incidentes de seguridad y Ciberseguridad?
9,2	NIST 27035:2023 MinTIC CIS V8	¿Se han asignado o definido roles y responsabilidades claves para los miembros del equipo de respuesta a incidentes?
9,3	CIS V8	¿Se tiene designado personal para administrar el manejo de incidentes?
9,4	CIS V8	¿Se tiene establecido datos de contacto para informar incidentes de seguridad?
9,5	NIST	¿Se realizan evaluaciones periódicas de riesgos para identificar posibles amenazas y vulnerabilidades que puedan dar lugar a incidentes de seguridad de la información?
9,6	Propio	¿Existe una definición de responsabilidades y procedimientos para los diferentes tipos de incidentes?
9,7	MinTIC	¿La Institución cuenta con herramientas y recursos adecuados para llevar a cabo las actividades de gestión de incidentes de acuerdo con las recomendaciones de la Guía del MinTIC?

Autor: propio consolidado de las normas (ANSI, 2023) (Center for Internet Security, 2021) (ISO/IEC 27001, 2022) (MinTIC, 2021) (NIST, 2020)

En el anexo A, se encuentra el nivel de cumplimiento detallado por cada control y sus observaciones, permitiendo tener la valoración inicial frente a la gestión de incidentes de Ciberseguridad.

9.1.3.2. Nivel de Cumplimiento

El nivel de cumplimiento se determina por varios estándares y prácticas que definen un nivel de madurez que ayudan a definir que tanto se está cumpliendo los controles y dar un calificativo para saber el nivel en el que se encuentra.

9.1.4. Conclusiones.

Con base en el análisis inicial se concluye lo siguiente:

- Se identifican falencias en la estructuración de los procesos ya que, aunque el proceso de tecnología está dentro el proceso de “Gestión Administrativa e infraestructura Física”, y es de apoyo no es visible para la organización.
- No se logrará estructurar el mapa de procesos ya que por políticas de la institución esto entraría en proceso de auditoría y actualmente no se cuenta con el capacity ni los recursos adecuados para este.
- El GAP o análisis de brecha que se definió para evaluar cómo está la organización, permite identificar cuáles son los puntos que se deben trabajar y empezar a mejorar con el fin de que se cumpla los estándares de la industria y sea eficiente.
- En los resultados iniciales se identifica que el proceso de gestión de incidentes de ciberseguridad se encuentra en un estado **Desconocido** siendo la escala más baja en el modelo definido y requiere una atención y visibilidad ante los Directivos.

9.2. DISEÑO DEL PROCESO DE GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD, PARA LA ENTIDAD ITFIP MEDIANTE LOS MODELOS Y LOS FRAMEWORK'S DE BUENAS PRÁCTICAS QUE PROPONE LA ISO 27035:2023, LA NIST 800-61 REV-2 Y LA GUÍA DE GESTIÓN DE INCIDENTES DEL MINTIC.

De acuerdo a los estándares o metodologías actuales que existen en el mercado tecnológico como son la NIST 800-61, (NIST, 2020) ISO 27035 versión 2023 (ANSI, 2023) y la guía de la Mintic – Gestión de Incidentes en su versión 2021 (MinTIC, 2021); se propone un documento en base a lo anterior respecto a la propuesta de la metodología de la “Gestión de Incidentes de Ciberseguridad para la ITFIP”, de la cual se estructura en una serie de premisas y factores clave para el correcto procedimiento que se debe tener en cuenta frente a una amenaza temprana en proceso respecto a los incidentes de Ciberseguridad.

Por otra parte, se da referencia la norma ISO 9001:2015 (Organización Internacional de Normalización (ISO, 2024), permite estructurar y documentar un procedimiento, se toma como referencia la siguiente estructura:

- Título
- Propósito
- Alcance
- Definiciones
- Responsabilidades

- Procedimiento
- Evaluación
- Referencias
- Documentación y registros
- Control de Cambios

Con base en la estructura mencionada anteriormente se logró definir la forma con la cual se va a trabajar el procedimiento de Gestión de incidentes de Ciberseguridad, además del documento del MinTIC que permite referenciar este marco ya que es el que mejor se acomoda al ITFIP por el tipo de entidad por ser publica y del sector gobierno vigilada por el ministerio de Educación el cual está bajo los lineamientos del MINTIC en temas de Seguridad y Tecnología.

Adicionalmente del modelo CCN-STIC 817 - Esquema Nacional de Seguridad (Centro Criptológico Nacional, 2020) se tomó como referencia las definiciones de:

- Clasificación de incidente de Ciberseguridad
 - Tipo de amenaza
 - Origen de la amenaza
 - Categoría
 - Taxonomía y clasificación de incidentes de ciberseguridad.

Anteriormente, estos permiten ayudar con el alcance de las terminologías y se adaptan a lo que busca el ITFIP para su guía y manual de proceso de gestión de incidentes de ciberseguridad.

Finalmente, el marco general que abarca todo el proceso y la guía de gestión de incidentes de ciberseguridad del ITFIP, se diseñó con base en la comparación de los diferentes marcos resaltados en el punto 5.4.7, está misma bajo la normativa de la NIST SP 800-61 (NIST, 2020) donde quedó plasmado todo el proceso de Gestión de Incidentes de Ciberseguridad del ITFIP, con cada uno de sus componentes, fases, métricas y comunicación, además de las definiciones y estructura que se propone en el modelo del CSIRT.

- 9.2.1. Documentarse sobre los frameworks ISO27035:2022, NIST 800-61 Rev-2 y la Guía de Gestión de incidentes de seguridad del MINTIC.

Se realiza una investigación y profundiza en cada uno de estos, los cuales están relacionados en el [MARCO TEORICO](#), para identificar como se pueden aplicar al sistema del ITFIP y cual se acomoda mejor, según las necesidades de la institución.

- 9.2.2. Generar entrevistas con las áreas que deberían estar a cargo del proceso de gestión de incidentes.

Para el proceso de gestión de incidentes, se realizan sesiones involucrando a las áreas y/o responsables de los procesos que conforman el grupo de trabajo en la atención de incidentes de ciberseguridad, así como lo referencia guía de la NIST

(NIST, 2020) en la sección de roles y responsabilidades; para esto se generó una propuesta de los cargos que deberían existir en el ITFIP para conformar un correcto grupo de gestión de incidentes, como se menciona en la tabla 8:

Tabla 8 Propuesta de cargos

Área o Cargo	Rol en el proceso
Tecnología	Contención y soporte en incidentes
Analista de Soporte	Recepción de reportes y primeros diagnósticos
Oficial de Seguridad	Coordinación Gestión de Incidentes
Coordinador de Redes	Análisis de tráfico y mitigación en la red
Asesor Legal- Gestión administrativa	Evaluación legal y soporte ante incidentes con impacto regulatorio
Analista de Riesgos- Calidad	Identificación de impacto y priorización de riesgos
Coordinadora de Comunicaciones	Manejo de la comunicación interna y externa
RRHH – Gestión Administrativa	Gestión de incidentes relacionados con personas internas
Gestión Administrativa - Continuidad	Apoyo en activación de planes de recuperación

Autor: Propio

Al identificar que el equipo de la institución no cuenta con todos los roles planteados anteriormente, se da alcance a las áreas que, si existen, se logró definir lo siguiente:

Objetivo de las sesiones: levantar información general sobre las funciones y responsabilidades de las áreas clave ante los incidentes de seguridad de la ITFIP, para construir un modelo de respuesta coordinado y efectivo.

Temas tratados con cada una de las áreas que participan en la gestión de incidentes.

- Comunicaciones: Las comunicaciones internas son reactivas y no siguen un protocolo formal, sin un proceso debido.
- Soporte técnico e infraestructura: TI ejecuta acciones rápidas, pero sin documentación estructurada.
- Asesor legal – Gestión administrativa: Área legal o jurídica participa en casos graves, definición de umbrales de la misma forma el impacto en la operación.
- Gestión administrativa – Continuidad: Proponer o generar un matriz de criticidad
- Gestión Administrativa - RRHH: Revisión al interior del protocolo disciplinario ante incidentes de ciberseguridad, en caso de que se presente el escenario de error humano.

Aportes de las áreas:

- Tecnología (Alcance Seguridad):
 - Disposición para formalizar procesos y documentar tiempos de respuesta, autoridad para coordinar incidentes entre las áreas involucradas.
 - Mapear incidentes según impacto reputacional y operacional.
- Gestión Jurídica: Definir cuando un incidente requiere notificaciones a entidades externas.

Recomendaciones de las Áreas:

- Crear un comité de respuesta a incidentes
- Establecer protocolos y roles claros por tipos de incidentes.
- Desarrollar simulacros y programas de concientización hacia los usuarios.
- Incorporar en el sistema Helpdesk el módulo centralizado de tickets de incidentes.

Acuerdos:

- Proponer una matriz de criticidad para ser validada a cargo de la gestión administrativa – riesgos.
- Proponer plantilla de protocolo de escalamientos, responsabilidad de TI y Seguridad.
- Evaluar y proponer simulacros y programas de concientización a cargo de gestión administrativa- Comunicaciones, Seguridad y continuidad.

Observaciones:

Existe una alta disposición de todas las áreas para colaborar en la construcción del modelo de gestión de incidentes de Ciberseguridad. Se identificó como prioridad establecer un marco de gobernanza y canales de reporte claros.

9.2.3. Verificar si se cuenta con la política o lineamientos asociados a la gestión de incidentes y actualizar o acompañar en su definición.

Acorde a las sesiones realizadas y en el levantamiento de información de los procesos de la ITFIP, la institución no cuenta a nivel de gobierno en seguridad de información con un Manual de seguridad y privacidad de la información abarcando lineamientos y políticas que rigen la normatividad para el cumplimiento de la protección de la información; de esta misma tampoco cuenta con la metodología y proceso para Gestión de Incidentes de Ciberseguridad que permita atender los incidentes de ciberseguridad que puedan presentarse en su infraestructura tecnológica, plataformas y demás servicios.

De acuerdo con lo anterior, se realiza acompañamiento para definir las políticas de Gestión de incidentes de Ciberseguridad diseñada para la ITFIP, en el contexto organizacional, académico y tecnológico, de acuerdo con la referencia que propone los estándares de la Gestión de Incidente de Ciberseguridad (ANSI, 2023), (MinTIC, 2021).

Política de Gestión de incidentes de Ciberseguridad.

La Política de Gestión de Incidentes de Ciberseguridad de la ITFIP establece los lineamientos y procedimientos para la preparación, detección y análisis, contención erradicación y recuperación y las actividades post-incidentes; relacionado con la seguridad de la información y los activos digitales de la institución. Esta política busca garantizar la continuidad operativa, proteger la confidencialidad, integridad y disponibilidad de la información, y cumplir con los requerimientos legales y normativos aplicables.

Objetivos:

- Detectar y registrar de forma oportuna cualquier evento de ciberseguridad que pueda afectar los sistemas informáticos, la red institucional, las plataformas educativas y los datos personales y académicos de los miembros de la comunidad educativa.
- Clasificar e investigar los eventos de seguridad para determinar su impacto potencial.
- Establecer mecanismos eficaces de respuesta y recuperación ante incidentes de ciberseguridad.
- Promover una cultura de seguridad informática entre el personal docente, administrativo, estudiantes y terceros.
- Documentar y analizar los eventos para prevenir su recurrencia y fortalecer los controles de seguridad.

Alcance:

Esta política aplica a todo el personal, estudiantes, proveedores, contratistas y cualquier tercero que utilice o tenga acceso a los recursos tecnológicos y sistemas de información de la ITFIP.

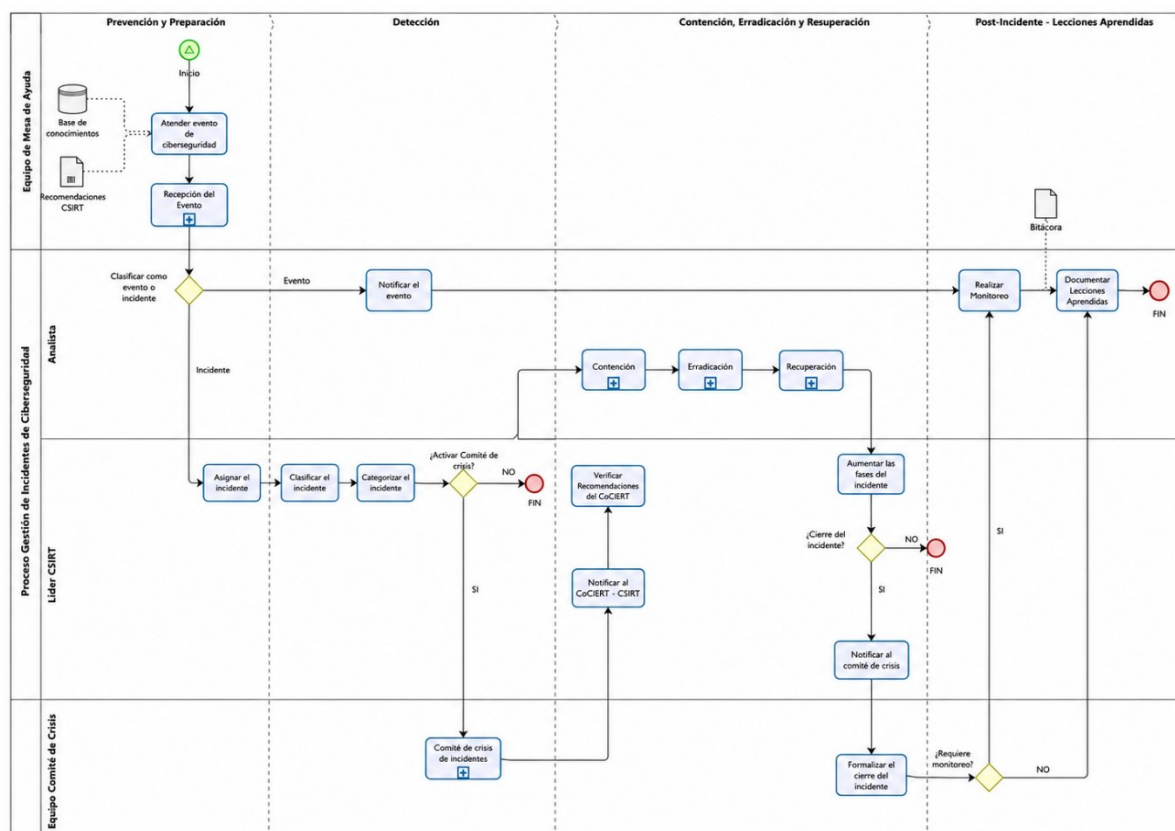
Lineamientos:

- Todos los usuarios son responsables de reportar cualquier evento de ciberseguridad.
- Cada evento debe ser registrado y documentado en un sistema de gestión de eventos de ciberseguridad.
- La atención de eventos de ciberseguridad debe ser gestionados por el equipo de tecnología.
- Las actividades post-incidentes que abarcan las lecciones aprendidas deben ser utilizadas para fortalecer las capacidades de respuesta, los mismos controles y políticas de la gestión de incidentes de ciberseguridad.

9.2.4. Propuesta del Diseño de la Gestión de Incidentes de Ciberseguridad de la ITFIP por etapas.

A continuación, se relaciona el diseño propuesto a la ITFIP de las etapas o fases definidas con base en lo plasmado por los diferentes marcos en especial el Mintic (MinTIC, 2021)

Ilustración 10 Diseño del Proceso Gestión de incidentes de Ciberseguridad



Autor: Propio.



GestionDelIncidente
s.png

El diseño propuesto hace referencia a varios marcos y estándares de referencia, en el cual se propone un modelo híbrido, haciendo énfasis en especial la metodología planteada por el MinTIC (MinTIC, 2021), pero en sus sub-ítems se tienen en cuenta temas de NIST (NIST, 2020), CIS (Center for Internet Security,

2021) y para los temas de concienciación y la ISO 27035:2023 (ANSI, 2023) en sus buenas prácticas.

9.2.5. Propuesta de los roles, responsabilidades y personal necesario por la atención de los incidentes de seguridad y Ciberseguridad.

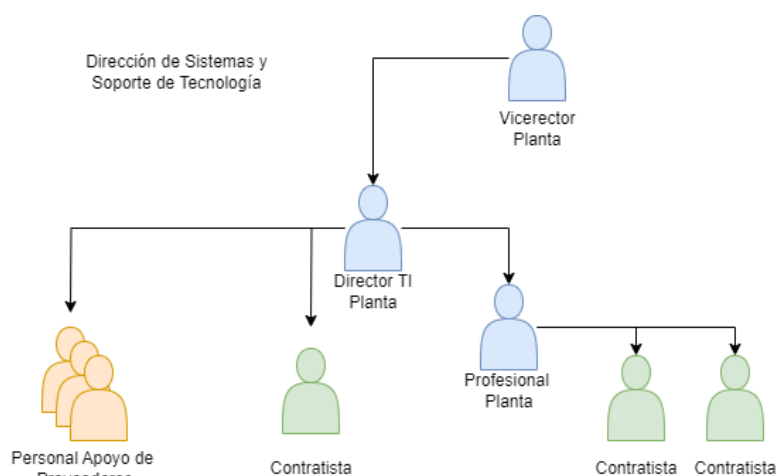
Para este punto, se realizó un análisis al interior de la institución, verificando la composición de la estructura del área de Tecnología, compuesta de la siguiente forma:

Estructura Actual:

Actualmente el ITFIP cuenta con personal reducido ya que su planta es pequeña y los apoyos son contratistas y proveedores que apoyan la operación y administración de las herramientas.

A continuación, se muestra el organigrama del área de TI con los contratistas y proveedores:

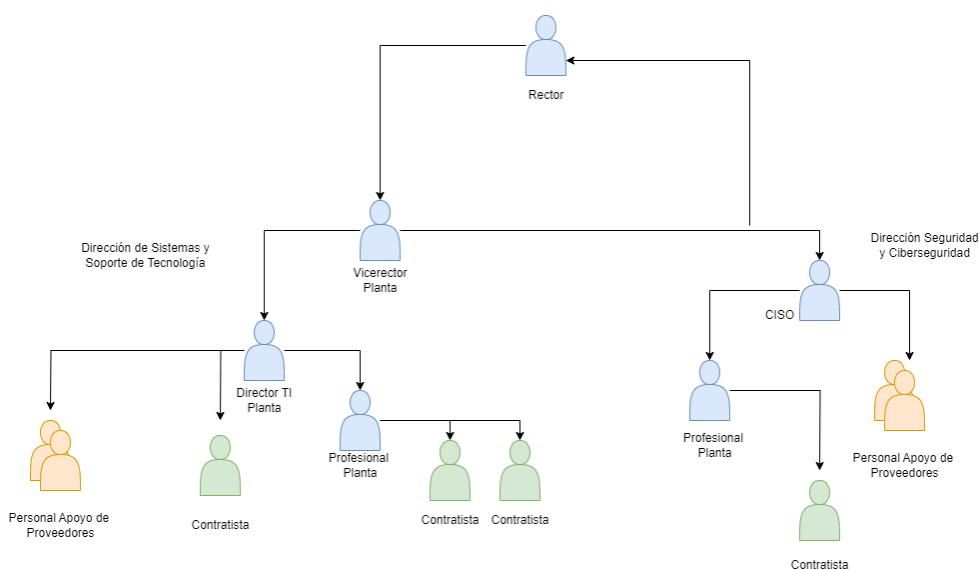
Ilustración 11 Estructura Actual



Autor: Propio con base en la información entregada por el ITFIP

Propuesta de personal Seguridad – Estructura Sugerida

Con base en lo identificado en la estructura organizacional actual del ITFIP se realizó un análisis de cómo debe quedar dividida el área de TI y de Ciberseguridad para operar de manera eficiente y se planteó la siguiente propuesta:

Ilustración 12 Estructura Propuesta

Autor: Propio con base en la información entregada por el ITFIP

Con base en los perfiles sugeridos, se detalla la estructura de cada perfil y la descripción de estos mismos actores que conforman e intervienen en el proceso de la Gestión de Incidentes de Ciberseguridad; detallando sus competencias, funciones y responsabilidades tal como se plasma en:

- Anexo D: Perfiles Sugeridos.
- Anexo E: Roles y Responsabilidades.

Estos roles y perfiles sugeridos, se planteó bajo el diseño anteriormente mostrado haciendo referencia a lo que plantea la metodología del Mintic. (MinTIC, 2021)

9.2.6. Propuesta de la matriz de escalamiento: interna y externa.

Tomando como referencia la metodología que propone la Mintic (MinTIC, 2021), se realiza un levantamiento de información abarcando la disponibilidad y existencia de toda relación con respecto a la infraestructura tecnológica tanto interno como externo de la ITFIP, incluyendo los proveedores de tecnología, servicios de alojamiento - Hosting, soporte técnico, encargados de tecnología, contactos legales, los gestores de respuesta incidentes, CSIRT, Seguridad informática, etc.; con el objetivo de garantizar un contacto y escalamiento oportuno y óptimo a la hora de un posible incidente de Ciberseguridad.

Respecto a la identificación del incidente referente a la guía del MinTIC en su versión 2021 indicando lo siguiente *“Una vez identificado el incidente de seguridad digital se deberá reportar ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno, los incidentes catalogados como Muy Grave y Grave por la entidad, para el respectivo apoyo y coordinación en la gestión de estos a través del formato de reporte establecido por el CSIRT Gobierno, el cual estará disponible por los canales de comunicación autorizados:*

Csirtgob@mintic.gov.co
01 8000 910742 - Opción 3.

“Los incidentes catalogados por el responsable de seguridad digital de la entidad, como Menos Grave y Menor, deben ser comunicados al CSIRT

Gobierno en el formulario establecido una vez sea gestionado, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos.” (MinTIC, 2021), la ITFIP toma como referente este mismo proceso de escalamiento y notificación ajustándose al debido proceso informado.

En este mismo ámbito en la propuesta de notificación, se rige de acuerdo con lo mencionado en el proceso descrito en los anexos:

Anexo E: Comunicación del Incidente – Interna y Externa

Anexo F: Flujo del Incidente y los Niveles de atención de un incidente de Ciberseguridad

Para esto se establece los teléfonos de contacto de las personas que deben ser notificadas de acuerdo con el tipo de incidente de ciberseguridad que se haya presentado. Anexo E. Matriz de Escalamiento

9.2.7. Propuesta de documentos clave que apoyan el proceso de gestión de incidentes.

La gestión efectiva de los incidentes de ciberseguridad, además de las políticas y procedimientos bien definidos: se necesita documentación estructurada que respalde cada etapa del proceso; existen unos documentos operativos que apoyan directamente la gestión de incidentes de ciberseguridad como los siguientes; así como lo referencia en la estándares y guías de la NIST SP800-61 contenido en el plan de gestión de incidentes de seguridad de la

información (NIST, 2020), ISO/IEC 27035 (ANSI, 2023) y la Mintic (MinTIC, 2021)

Registros y Bitácoras.

- Bitácoras e historial de incidentes: Documento de registro cronológico de los eventos, responsables y acciones tomadas; incidentes resueltos, es muy útil para el análisis de las tendencias presentadas y la mejora continua. Anexo B - Bitácora de incidentes

Formatos y plantillas:

- Formato de reporte de incidentes de ciberseguridad: Documento de registro de información esencial del incidente que incluye (fecha, hora, descripción, impacto, responsables, acciones tomadas, etc.) Este mismo usado para validación del estado del incidente, resuelto y la comunicación a los afectados o dueños. Anexo B - Formato para reportes de Incidentes de Ciberseguridad

Instructivo y guías:

- Formato de resolución rápida para incidentes de Ciberseguridad: Paso a paso detallado para resolver incidentes comunes; ayudan al equipo o personal a categorizar y priorizar los eventos o incidentes de ciberseguridad. Anexo B - Formato de resolución rápida para incidentes de Ciberseguridad.

- Check de Incidentes: Lista de chequeo para el manejo de incidentes de ciberseguridad en las etapas (antes, durante y después). Anexo B- Check de Incidentes.
- Checklist de verificación de servicios: Lista de chequeo para verificar el estado de salud de los sistemas después de la solución de un incidente. Anexo B – Formato Verificador de servicios post-Incidente de Ciberseguridad

Comunicación:

- Formato de comunicación del incidente, matriz de escalamiento: Proceso de instrucción indicando, quién, cuando, como escalar un incidente de ciberseguridad, Informar a los dueños del proceso o servicio, usuarios, clientes, proveedores sobre los incidentes relevantes. Anexo B – Formato de comunicación de incidentes de Ciberseguridad.
- Lista de contactos de emergencia: Documento matriz con los datos de los especialistas, proveedores, equipo de respuesta a incidentes. Anexo B – Formato matriz de contactos de emergencia.

Estos formatos e instructivos son esenciales para registrar eventos, guiar al equipo de gestión de respuestas a incidentes en la resolución de problemas y asegurar la trazabilidad de las acciones. Estos elementos permiten documentar incidentes, establecer lineamientos claros para su clasificación y escalamiento, así como evaluar el cierre y las lecciones aprendidas. Al implementar y

mantener estos registros, la ITFIP fortalecerá la capacidad de respuesta, también la optimización de los tiempos de recuperación y de esta forma promoverá la mejora continua en la gestión de servicios TI y sobre todo en la gestión de eventos de Ciberseguridad.

9.2.8. Proponer de métricas e indicadores de referencia, para la mejora continua.

Las métricas definidas para la gestión de incidentes de Ciberseguridad permiten que se pueda medir el proceso y la gestión de cada una de las etapas identificadas en la gestión de incidentes de ciberseguridad al interior de la institución y permite genera planes de mejora que ayuden a la mejora continua.

A continuación, se listan las métricas definidas:

- Tiempo de Respuesta del Incidente

Tabla 9 Indicador de Respuesta

Indicador	Tiempo de Respuesta del Incidente de Ciberseguridad.
Objetivo	Determinar el tiempo que toma el equipo en atender el incidente de ciberseguridad.
Medición	Promedio de la duración en minutos de cada incidente de ciberseguridad presentado desde el reporte hasta el cierre.

Caracterización	Se permite medir la eficiencia del equipo en la respuesta del incidente.
Frecuencia	Trimestral
Tipo	Métrica

Autor: Propio

- Cantidad de incidentes de Ciberseguridad resueltos o cerrados

Tabla 10 Indicador de Cantidad de Incidentes

Indicador	Cantidad de incidentes de Ciberseguridad resueltos o cerrados
Objetivo	Medir la cantidad de incidentes resueltos.
Medición	Cantidad de Incidentes resueltos o cerrados / Cantidad de Incidentes Reportados
Caracterización	Permite medir la capacidad del equipo para resolver los incidentes de ciberseguridad.
Frecuencia	Mensual

Tipo	Métrica
------	---------

Autor: Propio

- Incidentes de Ciberseguridad Falsos positivos

Tabla 11 Indicador Falsos Positivos

Indicador	Incidentes de Ciberseguridad Falsos positivos
Objetivo	Medir la cantidad de falsos positivos reportados para la gestión de incidentes.
Medición	Cantidad de Incidentes categorizados como falsos positivos / Cantidad de Incidentes Reportados
Caracterización	Permite identificar si se está realizando un adecuado reporte de los incidentes de ciberseguridad.
Frecuencia	Trimestral
Tipo	Métrica

Autor: Propio

9.2.9. Presentar diseño y propuesta a los directivos y responsables del proceso de gestión de incidentes del ITFIP.

De acuerdo con la presentación del diseño de gestión de incidentes de Ciberseguridad, socializado al equipo del ITFIP, se genera acta relacionada en el Anexo G, con el detalle de los alcances y acuerdos presentados.

9.2.10. Conclusiones

De acuerdo con el diseño del proceso de gestión de incidentes de ciberseguridad se concluye.

- Fortalecer la postura institucional de ITFIP en ciberseguridad, respecto al diseño metodológico representa un avance estratégico para la universidad en materia de seguridad de la información, al establecer un proceso formal, estructurado y alineado con estándares nacionales e internacionales ya expresados.
- El modelo propuesto ha sido adaptado considerando la naturaleza académica, investigativa y administrativa de la ITFIP, contemplando la participación de áreas involucradas y la necesidad de asegurar la continuidad de los servicios tecnológicos.
- Se ha definido una estructura funcional que asigna roles y responsabilidades específicas al personal involucrado en la gestión de incidentes de ciberseguridad, promoviendo una respuesta óptima y eficaz.
- La implementación del proceso permitirá minimizar los efectos negativos de los incidentes, reducir los tiempos de respuesta y recuperación, y prevenir recurrencias mediante el aprendizaje continuo.

- Este diseño contribuye al cumplimiento de obligaciones legales y regulatorias en materia de protección de datos y seguridad de los activos de informacion, lo que mejora la imagen institucional de la ITFIP ante la comunidad, el sector educacion y los entes de control.
- El éxito del proceso requiere el compromiso activo de la alta dirección educativa y el acompañamiento transversal de todas las areas o personal involucrados, incluyendo rectoría, areas académicas y administrativas.

9.3.PROCESO DE GESTION DE INCIDENTES DE CIBERSEGURIDAD PARA LA ENTIDAD ITFIP

En este capítulo se abordara lo contemplado para el proceso de Gestión de Incidentes de Ciberseguridad para la institución ITFIP, esto incluye el modelo de trabajo el cual se construye con base en las normas ISO/IEC 27035:2023, NIST 800-61 REV-2 Y LA GUÍA DEL MINTIC PARA LA GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD, en donde según las definiciones de la primera y la segunda nos permitirá enfocar y orientar las buenas prácticas en la gestión de incidentes, definiendo las diferentes fases que deben ser contempladas para una correcta gestión de incidentes de acuerdo con lo expuesto en la tabla del

numeral [5.4.7](#) y la última consolida las mejores prácticas de la primera y la segunda pero orientada a entidades públicas permitiendo tener un cumplimiento frente a lo exigido por el MinTIC como ente de referencia para lo relacionado a seguridad de la información y tecnologías de la Información.

LA GUÍA DEL MINTIC PARA LA GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD: Esta guía tiene como objetivo definir las buenas prácticas para establecer un proceso efectivo de gestión de incidentes de Ciberseguridad en las entidades públicas. En particular, el ITFIP se incluye en esta categoría al ser una universidad del estado, sujeta a la regulación del Ministerio de Educación. Además, debe cumplir con lo estipulado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) en relación con temas de tecnología y manejo de la información. Por esta razón, se toma como referencia esta guía, que proporciona un marco adecuado para implementar buenas prácticas, basándose también en los estándares internacionales ISO/IEC 27035:2023 y NIST 800-61 REV-2.

Es importante señalar que, aunque la implementación del proceso no eliminará por completo la ocurrencia de incidentes de seguridad, sí contribuirá a reducir su probabilidad y a optimizar el tiempo y gestión de estos. Actualmente, el ITFIP carece de referencias en este ámbito, por lo que la adopción de estas buenas prácticas permitirá mejorar la visibilidad en la gestión de incidentes. Esto no solo ayudará a prevenir la materialización de incidentes, sino que también fomentará un enfoque de mejora continua en los procesos de seguridad.

Actualmente el ITFIP, de acuerdo con el GAP ejecutado, se encuentra apenas en un **3%** de cumplimiento de un **100%**, claramente es un resultado claro frente a la importancia de emplear buenas prácticas en este proceso, con el fin de ayudar al proceso de Tecnología en el actual frente a un posible incidente de seguridad.

Con base en lo documentado anteriormente se trabajará en las siguientes etapas:

- 9.3.1. Definir formalmente las etapas de implementación que harán parte del proceso de gestión de incidentes de ciberseguridad. (Implementación).

Tabla 12 Etapas de Implementación

Objetivo	Etapas	Responsable	Fecha
Implementar el proceso de gestión de incidentes de seguridad y ciberseguridad con todo el flujo de trabajo, instructivos, formatos, anexos guías y definiciones de acuerdo con el diseño que adopte el ITFIP para que el equipo de tecnología pueda actuar correctamente ante un incidente de seguridad cibernético.	Formalizar la matriz de roles y responsabilidades del proceso de gestión de incidentes de ciberseguridad.	Tecnología	05/08/2024 a 30/08/2024
	Formalizar e implementar la matriz de escalamiento interna y externa que fueron definidas para el proceso de gestión de incidentes de seguridad y ciberseguridad, para su publicación.	Tecnología	05/08/2024 a 30/08/2024
	Formalizar e implementar los documentos propuestos para apoyar el proceso de gestión de incidentes de ciberseguridad, incluyéndolos en el sistema de calidad para su seguimiento.	Alta Gerencia Tecnología Procesos	05/08/2024 a 13/09/2024
	Implementar y formalizar el reporte de métricas definidas para medir el proceso de gestión de incidentes de ciberseguridad, con los responsables de su medición y reporte.	Tecnología	16/09/2024 a 27/09/2024
	Verificar que cada una de las fases propuestas estén implementadas y validar los ajustes correspondientes.	Tecnología	30/09/2024 a 29/11/2024

	Generar acta de cierre de implementación del proceso de gestión de incidentes de seguridad y ciberseguridad para su publicación y cumplimiento.	Alta Gerencia Tecnología	Pendiente
--	---	--------------------------	-----------

Autor: propio

Con Base en la hoja de ruta de la tabla X relacionada anteriormente, se realizará el proceso de implementación de lo descrito en el punto [9.2](#) frente al diseño del proceso.

9.3.2. Formalizar la matriz de roles y responsabilidades del proceso de gestión de incidentes de ciberseguridad. (Implementación)

El ITFIP, al no contar con un proceso establecido para la seguridad informática y la gestión de la información, no tiene definido una matriz de roles y responsabilidades para la atención de incidentes de ciberseguridad. Sin embargo, considerando su estructura organizacional y el hecho de que la institución solo dispone del proceso de Tecnología, se han incluido los roles actuales que pueden contribuir desde la identificación hasta el cierre de los incidentes.

Para este proyecto de grado, se tomó como referencia la guía del MinTIC (MinTIC, 2021), en relación con los roles, y se definieron en función de la plantilla actual proporcionada. No obstante, también se recomienda la inclusión de futuros perfiles de acuerdo con el organigrama propuesto.

Estructura del CSIRT: El equipo de respuesta a incidentes del ITFIP debe estar conformado principalmente por el CISO/Líder del CSIRT, acompañado por personal designado de las siguientes áreas de Tecnología, Comunicaciones, Legal, y la Alta

Dirección, el detalle de esta información se encuentra en el Anexo E de este documento en el apartado roles y perfiles.

9.3.3. Formalizar e implementar la matriz de escalamiento interna y externa que fueron definidas para el proceso de gestión de incidentes de ciberseguridad, para su publicación. (Implementación).

La matriz de escalamiento es una herramienta crítica en la gestión de incidentes de ciberseguridad, ya que permite una respuesta efectiva que mitiga riesgos y protege los activos digitales del ITFIP. Aunque la institución ha identificado la matriz de escalamiento desde la perspectiva de soporte y atención para garantizar la disponibilidad, no se ha contemplado su aplicación específica para la atención de incidentes de ciberseguridad.

Para abordar esta necesidad, se ha tomado como referencia la normativa de (NIST, 2023), que establece un marco claro para la comunicación durante los incidentes de ciberseguridad. Esto mejora la eficiencia del proceso al definir roles y responsabilidades de manera precisa. Además, la (ANSI, 2023) proporciona directrices para la priorización de incidentes, asegurando que se asignen recursos de manera adecuada según la gravedad de cada situación.

Por otro lado, la guía del MinTIC (MinTIC, 2021) enfatiza la importancia de la mejora continua en la gestión de incidentes. Esta guía facilita la documentación y el análisis de incidentes, lo que permite aprender de cada experiencia y optimizar las respuestas futuras.

En cuanto a la matriz de escalamiento de nivel externo, es fundamental considerar las recomendaciones del (NIST, 2020) y (MinTIC, 2021), que promueven un proceso de gestión de incidentes que fomenta la comunicación y colaboración con entidades externas, como COLCERT que son expertos en ciberseguridad para atención de incidentes de

ciberseguridad. Esta colaboración es crucial para obtener apoyo adicional durante un incidente y mejorar la capacidad de respuesta, beneficiando no solo al ITFIP, sino también a otras instituciones del sector académico mediante un esfuerzo conjunto.

La documentación de los dos escenarios se relaciona en el anexo E y F de este documento, permitiendo identificar el proceso de la comunicación para trabajar sobre los incidentes de ciberseguridad establecidos para el ITFIP.

9.3.4. Formalizar e implementar los documentos propuestos para apoyar el proceso de gestión de incidentes de ciberseguridad, incluyéndolos en el sistema de calidad para su seguimiento. (Implementación).

Con base en los documentos de referencia, como resultado del proyecto de grado se ha elaborado un documento que detalla la estructura el proceso de gestión de incidentes de ciberseguridad para el ITFIP. Este documento está organizado de la siguiente manera:

Introducción Presentación del contexto y la importancia de incidentes de Ciberseguridad en el ITFIP con base en (NIST, 2020)

Descripción Proceso: Detalle de cómo se definió el proceso basado en la guía de (MinTIC, 2021)

Objetivo: Definir el objetivo del proceso, basado en lo documentado del (MinTIC, 2021).

Alcance: Limitado a incidentes de Ciberseguridad basado en lo recomendado por la (MinTIC, 2021).

Referencias: Este apartado proporciona una lista de documentos y normativas que fundamentan el proceso de gestión de incidentes. Su propósito es asegurar que el

proceso esté alineado con las mejores prácticas y estándares reconocidos, lo que refuerza su validez y efectividad. (MinTIC, 2021).

Guías: Ofrecer directrices y recomendaciones que orienten la implementación del proceso de gestión de incidentes, facilitando la adopción de prácticas efectivas y coherentes. Con base en (ANSI, 2023) (NIST, 2020) (MINTIC, 2016) (MinTIC, 2021).

Términos y definiciones: Aclarar los términos técnicos utilizados en el contexto de la gestión de incidentes según (ISO/IEC, 2022).

Clasificación de incidentes de Ciberseguridad: Permitir a las organizaciones priorizar su respuesta y asignar recursos de manera adecuada, facilitando la identificación y gestión de incidentes según su naturaleza y gravedad según (Centro Criptológico Nacional, 2020).

- Tipo de Amenaza
- Origen de la Amenaza
- categoría
- Perfil del Usuario

Requerimientos Legales: Detallar las obligaciones legales que las instituciones deben cumplir en relación con la gestión de incidentes, garantizando que las prácticas estén alineadas con la legislación vigente y promoviendo la responsabilidad. (Centro Criptológico Nacional, 2020) (MinTIC, 2021) (COLCERT, 2023).

Taxonomía de la clasificación de incidentes de ciberseguridad: Proporcionar un marco para categorizar los incidentes de ciberseguridad (Centro Criptológico Nacional, 2020) (MinTIC, 2021).

CSIRT: Describir el equipo de Respuesta a Incidentes según lo menciona (MINTIC, 2016) (MinTIC, 2021).

- Estructura CSIRT
- Líder CSIRT

Roles y Responsabilidades: Establecer claridad en las funciones de cada miembro del equipo de gestión de incidentes basado en (MinTIC, 2021).

- CISO
- Director de TI
- Líder Mesa de ayuda
- Administrador de Plataforma/Aplicación
- Usuario Final
- Responsable Jurídico
- Líder de Comunicaciones

Etapas del Incidente: Proporcionar un marco claro que guíe a los equipos a través de cada fase del ciclo de vida de un incidente, desde la identificación hasta la recuperación como lo estipula (MinTIC, 2021) (NIST, 2020)

- Prevención y preparación
- Detección
- Contención Erradicación y Recuperación
- Actividades Post Incidentes-Lecciones Aprendidas
- Diagrama de Etapas Definidas para la Gestión de Incidentes de Ciberseguridad
- Medición (Autores)

Comunicación del Incidente: Protocolos de comunicación que aseguren que la información fluya de manera adecuada y oportuna durante un incidente de acuerdo con (MinTIC, 2021) (Autores).

- Interna
- Externa
- Matriz

Control de Cambios: Establecer un procedimiento para gestionar y documentar los cambios realizados en el proceso de gestión de incidentes. Basado en lo definido en la (Organización Internacional de Normalización (ISO, 2024) (Autores)

Definir una estructura clara y bien organizada para el proceso de gestión de incidentes de ciberseguridad es fundamental para cualquier institución que busque proteger sus activos digitales y garantizar la continuidad de sus operaciones, en caso de una anomalía. Esta estructura proporciona un marco sistemático que permite a los equipos del ITFIP responder de manera efectiva y coordinada ante incidentes, minimizando su impacto y facilitando la recuperación. Sin embargo, se requiere un proceso de capacitación oportuno para desarrollarlo de la mejor manera.

Para obtener información detallada sobre el contenido del documento completo y sus documentos de apoyo, se recomienda consultar los siguientes anexos:

- Anexo B
- Anexo C
- Anexo D
- Anexo E
- Anexo F

Propósito: Estos anexos proporcionan información complementaria y específica que respalda y amplía los conceptos presentados en el documento principal del Anexo E, facilitando una comprensión más profunda del proceso de gestión de incidentes de ciberseguridad.

9.3.5. Implementar y formalizar el reporte de métricas definidas para medir el proceso de gestión de ciberseguridad, con los responsables de su medición y reporte. (Implementación).

El ITFIP, al no contar con un proceso formal de gestión de incidentes de ciberseguridad, carecía de métricas asociadas a la gestión de incidentes. A diferencia de las métricas generadas por herramientas como Fortinet, las cuales no fueron documentadas ni medidas, esta situación limitaba la capacidad de la institución para evaluar y mejorar su respuesta ante incidentes.

Con el objetivo de establecer un marco de referencia para la gestión de incidentes, se han definido tres métricas principales que deben ser implementadas al inicio del proceso. Estas métricas permitirán no solo medir la efectividad de la gestión de incidentes, sino también facilitar la mejora continua a medida que el ITFIP desarrolle su nivel de madurez en este ámbito.

- Tiempo de Respuesta del Incidente de Ciberseguridad: Permitirá a los equipos a identificar cuanto se están tardando en cada una de las fases y aplicar procesos de mejora continua, para respuestas efectivas.
- Cantidad de incidentes de Ciberseguridad resueltos o cerrados: Permite identificar al equipo el estado actual de incidentes identificados y su estado.

- Incidentes de Ciberseguridad Falsos positivos: Permite identificar que tan mal informados están los usuarios en el reporte de posibles incidentes y definir un mejor triage para categorización.

Finalmente, para ver la hoja de vida estructura y formula de medición de cada indicador remitirse al Anexo E en el apartado de Medición.

9.3.6. Generar acta de cierre de implementación del proceso de gestión de incidentes de ciberseguridad para su publicación y cumplimiento. (Implementación).

De acuerdo con el anexo H, se define acta

9.3.7. Conclusiones.

De acuerdo con el proceso de implementación se concluye lo siguiente:

- Se logró la creación y formalización de la matriz de roles y responsabilidades, lo que ha permitido clarificar las funciones de cada miembro del ITFIP a pesar del poco personal, en la gestión de incidentes de ciberseguridad. Esto ha mejorado la comunicación y la colaboración entre los equipos, asegurando que cada persona sepa y conozca el papel en la respuesta a incidentes.
- La matriz de escalamiento, tanto interna como externa, fue formalizada e implementada con éxito. Esto ha facilitado una

respuesta más ágil y efectiva ante incidentes, garantizando que los problemas sean escalados a los niveles adecuados de gestión y que se sigan los protocolos establecidos para la comunicación externa.

- Se formalizaron e implementaron los documentos de trabajo necesarios para apoyar el proceso de gestión de incidentes de ciberseguridad. Esto ha permitido un seguimiento más riguroso y una mejora continua en los procesos, sin embargo, se requiere integrar al sistema de procesos de calidad interno.
- Se implementó un sistema de reporte de métricas/indicadores que mide la efectividad del proceso de gestión de incidentes de ciberseguridad. Los responsables de la medición y el reporte han sido designados, lo que permitirá empezar a obtener datos precisos y relevantes para la toma de decisiones y la mejora del proceso.

Finalmente, la formalización de roles, la implementación de matrices de escalamiento, la creación de documentos de apoyo del proceso, el establecimiento de métricas y la verificación de procesos han permitido tener la gestión de incidentes de ciberseguridad en el ITFIP, ya que no existía. Esto permite una respuesta más ágil y efectiva ante posibles incidentes, mejorando la seguridad y resiliencia de la organización frente a las diversas amenazas cibernéticas a la que puede estar expuesta.

9.4. PLAN DE CONCIENTIZACIÓN DE LA GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD

Capacitar el personal sugerido y el propuesto por los directivos del ITFIP en todas las fases del proceso de la gestión de incidentes de ciberseguridad, por medio de un plan de concientización, que permita a toda la institución educativa saber cómo actuar, a quien reportar y que acciones tomar ante los diferentes escenarios de un incidente de seguridad.

9.4.1. Propuesta Plan de Concienciación

“El programa de concienciación de ciberseguridad y seguridad en general es un programa formal con el objetivo de capacitar a los usuarios sobre las posibles amenazas a la información de una organización y cómo evitar situaciones que puedan poner en riesgo los datos de la organización.”¹⁴

El presente plan aplica para los empleados de la entidad del ITFIP, estudiantes y proveedores, es extensivo para las personas que, por sus funciones y relaciones con la organización, compartan, utilicen o consulten información, así como las entidades de control internas o externas que tengan que ver o relacionarse con un incidente de ciberseguridad.

¹⁴ ¿Qué es un Plan de Concienciación de Seguridad informática? –. (2021, julio 26). AMITI.
<https://amiti.org.mx/7719/plan-concienciacion-seguridad-informatica>

El plan principalmente se enfoca en explicar y concientizar a las partes interesadas en cómo se debe gestionar un incidente de ciberseguridad y riesgos en los que pueden incurrir por el desconocimiento de estos temas. También se busca que, a través del conocimiento adquirido, sean partícipes en el apoyo y uso de buenas prácticas para mantener a salvo los activos informáticos, ya que las personas son el eslabón más débil y por ende puede ingresar las falencias de ciberseguridad.

Como referente para la adopción del plan de concienciación se toma como referente el marco NIST 800-50 “Building and Information Technology Security Awareness and Training Program “ (NIST, 2003), el cual permite estructurar el plan de concienciación en este caso enfocado a tomar la parte de incidentes de ciberseguridad y temas a fines para el entendimiento de esta temática. Con base en las recomendaciones expuestas por la NIST 800-50, se tomaron algunos puntos relevantes para tener como guía, se debe tener en cuenta lo siguiente para estructurar el plan:

- Objetivos
- Alcance
- Público objetivo
- Planificación
- Temas para tratar
- Material de Apoyo (Digital, Físico)
- Moderadores o Expertos en la temática
- Comunicación
- Ejecución
- Medición

9.4.2. Objetivos

- Definir un plan de concienciación para estudiantes, empleados y terceros que tengan relación con el ITFIP para la identificación, reporte y gestión de un incidente de ciberseguridad.
- Mencionar los principales ataques informáticos que existen.
- Capacitar y evaluar al personal definido por el ITFIP para que asuman la responsabilidad de reportar de manera oportuna cualquier incidente de ciberseguridad.
- Socializar la guía y manual de procedimiento de la gestión de incidentes de Ciberseguridad al personal de TI y demás involucrados

9.4.3. Alcance

El plan de concienciación está diseñado y centralizado para el área de TI, y demás personal del ITFIP que esté involucrado en un incidente de ciberseguridad, que permita que se dé una adecuada gestión a los incidentes de ciberseguridad y minimizar los impactos que pueda generar a la institución.

9.4.4. Público Objetivo

El plan de concientización se enfoca en todo el personal del ITFIP que participe en cualquiera de las fases definidas de un incidente de ciberseguridad, desde su reporte o identificación hasta su cierre y generación de informes y reporte de lecciones aprendidas. A continuación, se mencionan algunos de ellos:

- Estudiantes
- Trabajadores de Planta del ITFIP.
- Contratistas del ITFIP
- Proveedores del ITFIP
- Entre otros.

9.4.5. Temas

Los temas definidos para trabajar en el plan se identificaron del análisis previo (GAP o análisis de brecha) realizado al ITFIP sobre todo lo relacionado con incidentes de ciberseguridad. A continuación, se relaciona las temáticas:

- Definiciones y terminologías: En este punto se tratará los temas como que es un incidente, como se reporta, como identifico, que tipos de incidentes hay, que es un ataque cibernético, etc.
- Dar a conocer los responsables del CSIRT interno y el líder con las fases de como activar el equipo responsable de mitigar un incidente de seguridad.

- Dar a conocer las Fases de la gestión de incidentes de Ciberseguridad:
 - Preparación y prevención,
 - Detección,
 - Contención Erradicación y Recuperación
 - Activación Post incidente -Lecciones Aprendidas.
- Taxonomía adoptada para clasificar un incidente de Ciberseguridad.
- Canales de comunicación de incidente de ciberseguridad a nivel interno y externo del ITFIP.
- Importancia de documentar e identificar todo el flujo de incidente de ciberseguridad.
- Charlas por expertos en temáticas como: Ingeniería social, Malware, Riesgos, Buenas prácticas, controles y mitigaciones

9.4.6. Material de Apoyo

El material de apoyo será digital, donde se definirán presentaciones graficas por parte de los ponentes para la presentación de los temas propuestos en el punto anterior.

Se generarán infografías que serán entregadas por mail y puesto como fondo de pantalla por Active Directory a nivel interno a todo el personal definido por el ITFIP.

Con el Web Master se cargaron POP-UP a la intranet para que se recuerde los temas relevantes de la gestión de incidentes cibernéticos al interior del ITFIP.

Finalmente se compartirán páginas y sitios de apoyo con información relevante para los equipos de TI, como suscripciones a INCIBE, para recibir reportes diarios de temas cibernéticos y estar actualizados.

9.4.7. Responsables

Los moderadores serán personal externo a la institución, pero una vez el equipo de TI este totalmente capacitado este será el responsable de transmitir y reforzar la información al interior del ITFIP.

El responsable de guiar y alimentar el plan de gestión de incidentes de ciberseguridad es el CISO – Líder de Gestión de incidentes o responsable a cargo de asumir estos roles.

9.4.8. Comunicación

El plan de comunicación del plan de gestión de incidentes se da inicialmente por el área de TI con apoyo del área de comunicaciones, con el fin de que todo el personal interno y externo además de los estudiantes conozcan que existe el plan su objetivo alcance y cronograma para que puedan participar de este y estén informados de manera adecuada.

La comunicación se realizará por medio de:

- Mail
- Posters
- Pop-up en la página web.
- Promovido por el área de TI en los diferentes escenarios.

9.4.9. Ejecución

Para la ejecución e implementación del plan se definió sobre cada tema una periodicidad y el medio de ejecución ya que el responsable de toda la gestión es el CISO o quien asuma este Rol, a continuación, el detalle:

Tabla 13 Capacitaciones de concientización

Tema	Periodicidad	Medio
Definiciones y terminologías: En este punto se tratará los temas como que es un incidente, como se reporta, como identifico, que tipos de incidentes hay, que es un ataque cibernético, etc.	Semestral	Capacitaciones e infografías
Dar a conocer los responsables del CSIRT interno y el líder con las fases de como activar el equipo responsable de mitigar un incidente de seguridad.	Semestral	Capacitaciones e infografías
Dar a conocer las Fases de la gestión de incidentes de Ciberseguridad: Preparación y prevención, Detección, Contención	Anual	Capacitaciones

Erradicación y Recuperación, Activación Post incidente -Lecciones Aprendidas.		
Taxonomía adoptada para clasificar un incidente de Ciberseguridad.	Semestral	Capacitaciones e Infografías
Canales de comunicación de incidente de ciberseguridad a nivel interno y externo del ITFIP.	Mensual	Mail e Infografías
Importancia de documentar e identificar todo el flujo de incidente de ciberseguridad.	Semestral	Capacitaciones
Charlas por expertos	Anual	Conferencias especializadas

Fuente: Autores

9.4.10. Medición

Para la medición y evaluación de la efectividad del plan se definieron las siguientes métricas:

Tabla 14 Indicador de Efectividad -concientización

Indicador	Efectividad de las Capacitaciones
Objetivo	Evaluar la efectividad de las capacitaciones.
Medición	Cantidad de personal con evaluación aprobada / cantidad de Personal que realizo la evaluación
Caracterización	Permite saber si la estrategia definida es buena y aplicar mejoras al proceso.
Frecuencia	Trimestral
Tipo	KPI

Fuente: Autores

Tabla 15 Indicador de Participación -concientización

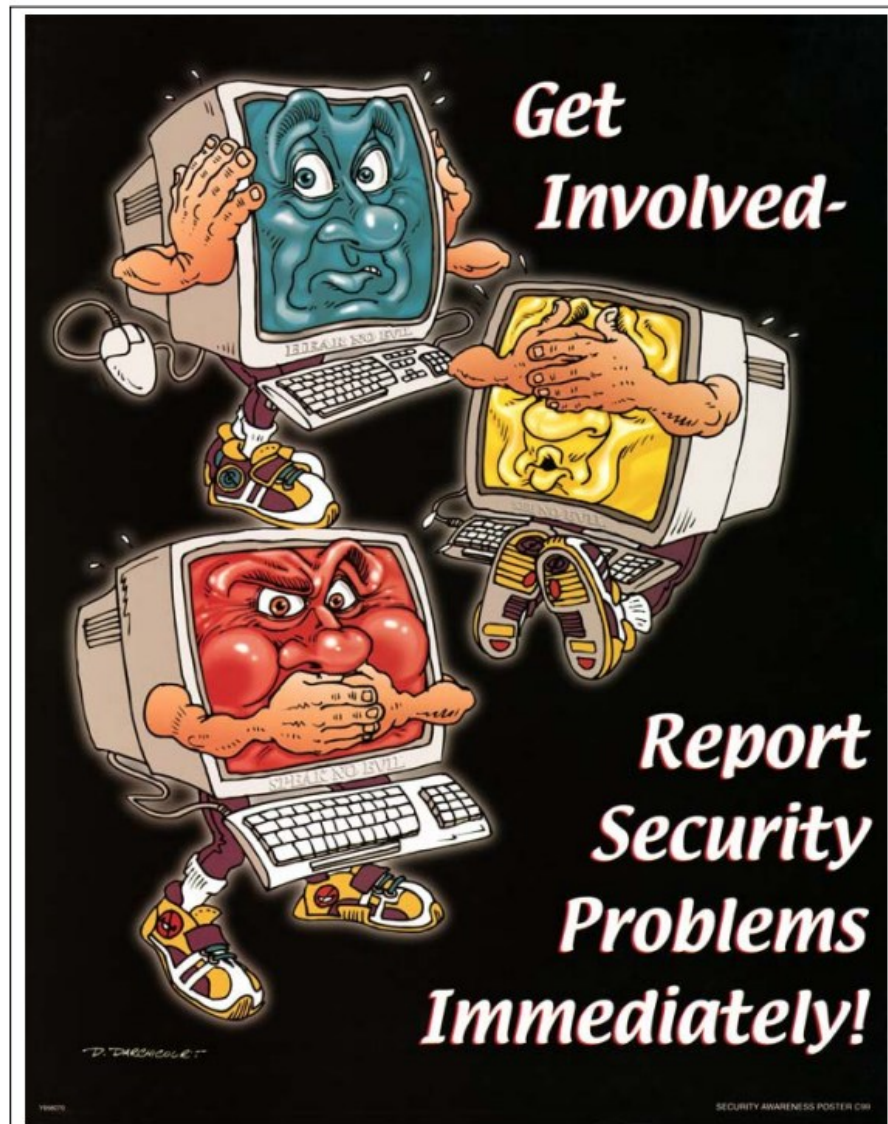
Indicador	Participación del Público Objetivo en plan de concientización
Objetivo	Medir que porcentaje está asistiendo a las charlas y capacitaciones definidas
Medición	Cantidad de personal asistente / Cantidad de personal programado
Caracterización	Permite saber la participación del público objetivo de cada capacitación.
Frecuencia	Trimestral
Tipo	KPI

Fuente: Autores

9.4.11. Anexos Plan de concientización

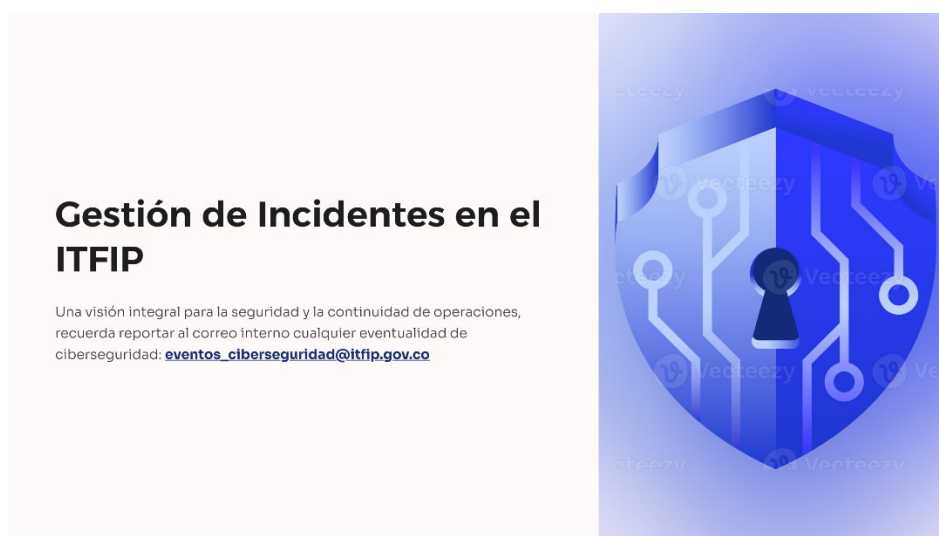
Infografías aplicables sobre cada una de las temáticas de acuerdo con las recomendaciones de NIST 800-50 y lo propuesto al ITFIP:

Ilustración 13 Infografía según NIST



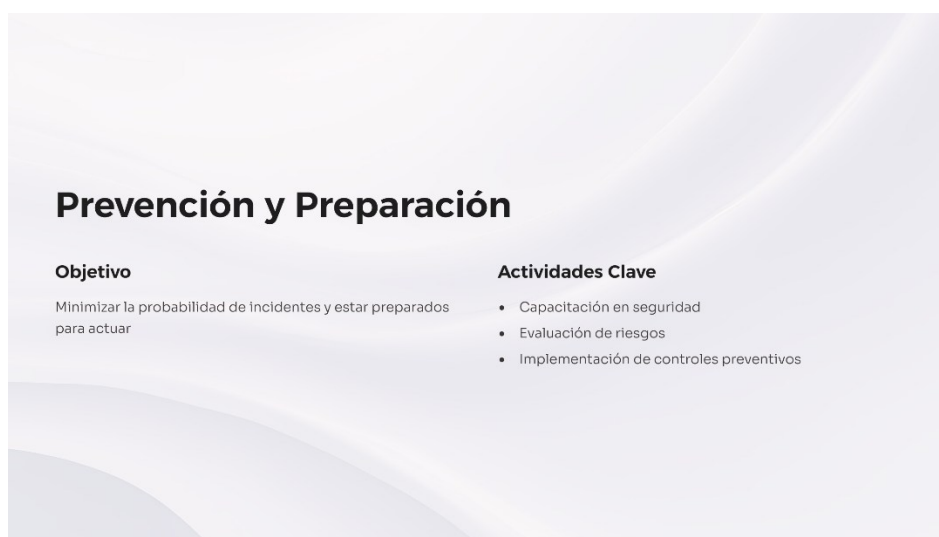
Autor: (NIST, 2003)

Ilustración 14 Pieza Informativa



Autor: Propio Ayuda IA

Ilustración 15 Pieza Informativa del Proceso



Propio Ayuda IA

Ilustración 16 Pieza Informativa



Autor: propio Ayuda de la IA

9.4.12. Crear campañas de concienciación para todo el alumnado, personal administrativo y docente del ITFIP sobre como reportar y actuar ante un incidente de ciberseguridad.

De acuerdo con el plan de concienciación en el punto 9.4.9 en el apartado **Ejecución** se detallan las campañas de concienciación que fueron definidas y que se aplicaran en la institución para las mejoras del proceso de gestión de incidentes de Ciberseguridad.

9.4.13. Dar recomendaciones y sugerencias sobre la importancia de la seguridad y ciberseguridad a nivel institucional.

La seguridad y ciberseguridad a nivel institucional son pilares fundamentales para salvaguardar la integridad, confidencialidad y

disponibilidad de la información. En un contexto donde las amenazas cibernéticas evolucionan constantemente y se vuelven más sofisticadas e indetectables, es responsabilidad que las instituciones adopten un enfoque proactivo permitiendo la implementación de políticas y procedimientos específicamente cuando es gestión de incidentes de ciberseguridad. Al priorizar la ciberseguridad, el ITFIP no solo protegen sus activos, sino que también cumplen los temas regulatorios exigidos por el MinTIC, para garantizar la seguridad de la información de estudiantes, docentes y administrativos.

Asimismo, la ciberseguridad debe ser considerada como un componente integral de la estrategia organizacional y debe ser transversal promoviendo una cultura de seguridad que involucre a todos los niveles de la institución, desde la alta dirección hasta los estudiantes. Esto implica la implementación de herramientas tecnológicas.

Las recomendaciones incluyen la creación de un equipo de respuesta a incidentes, la realización de simulacros de ciberseguridad y la colaboración interinstitucional como el

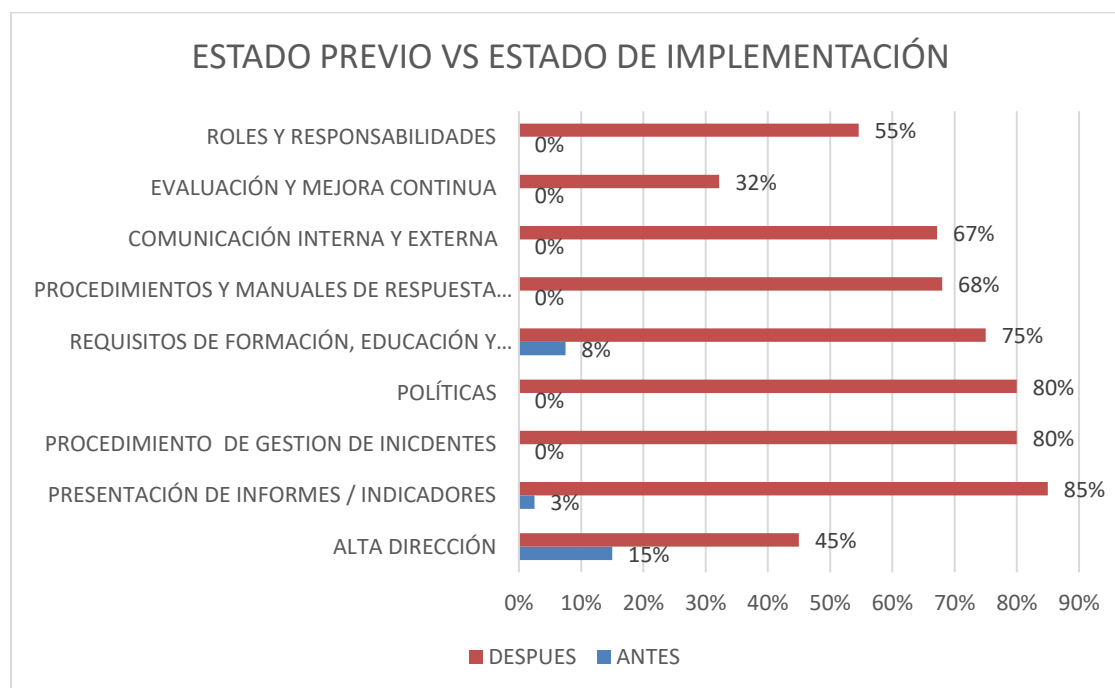
. El ITFIP pueden no solo mitigar riesgos, sino también responder de manera efectiva a incidentes, garantizando así la continuidad de sus operaciones en un entorno digital para sus estudiantes.

9.5.ANALISIS DE RESULTADOS

9.5.1. Conclusión de resultados del antes y después del proceso de gestión de incidentes de Ciberseguridad.

De acuerdo con el GAP relacionado en los anexos con el numeral 14.1, donde se realizó una primera valoración del ítem, se identificó que la entidad está en un nivel casi nulo frente a un proceso de gestión de incidentes de Ciberseguridad, previo a la implementación, como se demuestra en la siguiente ilustración:

Ilustración 17 Estado antes y después



Fuente: Autor

Los dominios que se evaluaron para identificar el nivel de madurez y estado actual frente a la implementación, según los marcos de referencia mencionados en los puntos anteriores, fueron los siguientes:

Tabla 16 Definición de pesos por dominio

Ítem	Dominios	%
1	ALTA DIRECCIÓN	10%
2	PRESENTACIÓN DE INFORMES / INDICADORES	10%
3	PROCEDIMIENTO DE GESTION DE INCIDENTES	10%
4	POLÍTICAS	10%
5	REQUISITOS DE FORMACIÓN, EDUCACIÓN Y SENSIBILIZACIÓN	10%
6	PROCEDIMIENTOS Y MANUALES DE RESPUESTA EN EL MANEJO DE INCIDENTES	20%
7	COMUNICACIÓN INTERNA Y EXTERNA	10%
8	EVALUACIÓN Y MEJORA CONTINUA	10%
9	ROLES Y RESPONSABILIDADES	10%

Autor: Propio.

Con base a los dominios definidos y a su peso frente al modelo evaluado, se tuvo en cuenta la siguiente tabla, que permite determinar el estado actual del proceso:

Tabla 17 Nivel de cumplimiento

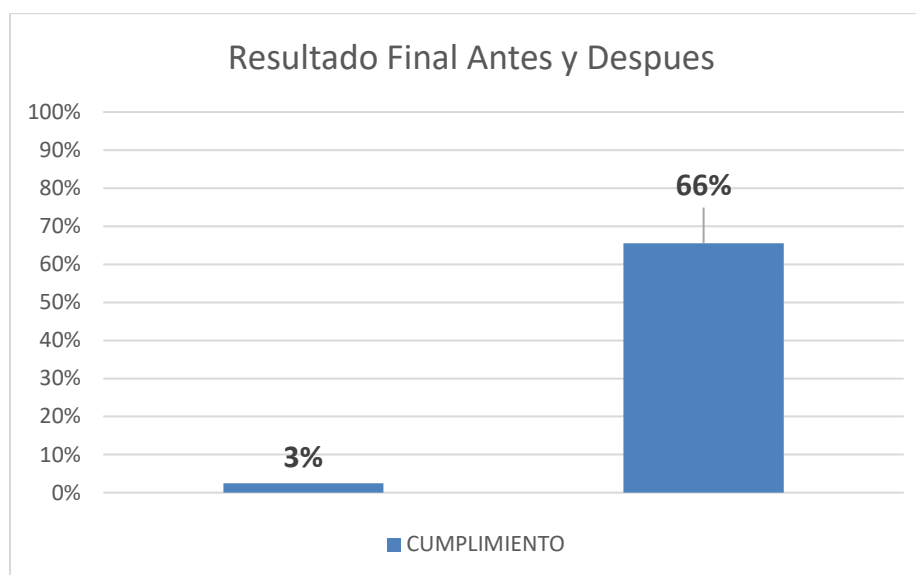
Estado	Descripción	Margen Inicial	Margen Final
Desconocido	No ha sido siquiera revisado aún	0%	10%
Inexistente	Ausencia completa de una política, procedimiento, control, etc. legibles	11%	15%
Inicial	El desarrollo apenas ha comenzado y requerirá un trabajo significativo para satisfacer los requisitos	16%	25%
Limitado	Progresando bien pero no completado aún	26%	35%
Definido	El desarrollo está más o menos completo, aunque con ausencia de detalles y/o no está aún implementado, en cumplimiento vigente ni activamente avalado por la alta dirección.	36%	45%
Gestionado	El desarrollo está completo, el proceso / control ha sido implementado y recientemente comenzó a operar	46%	70%
Optimizado	El requisito está plenamente conforme, está plenamente operativo como se espera, está siendo activamente supervisado y mejorado, y hay evidencia sustancial para demostrar todo lo antedicho a los auditores	71%	90%
No Aplica	TODOS los requerimientos en el cuerpo principal de la norma ISO/IEC 27001 son obligatorios SI su SGSI va a ser certificado. Caso contrario, la gerencia a cargo, puede ignorarlos	91%	100%

Autor: Adoptado de marco de madurez.

Adicionalmente, se logra obtener resultados positivos, después de estar en un margen **Desconocido**, como se evidencia en la tabla anterior “No ha sido revisado aún”, haciendo referencia al proceso de Gestión de Incidentes de Ciberseguridad, el logro fue subir de un **3%** a un **66%** de cumplimiento frente al modelo evaluado inicialmente estando en un nivel **Gestionado** “El desarrollo está completo, el proceso / control ha sido implementado y recientemente comenzó a operar”, como es común en estos procesos siempre se va requerir una mejora continua para que este permita obtener mejores prácticas e identificar falencias en el proceso.

A continuación, se relacionan los resultados descritos anteriormente:

Ilustración 18 Resultados



Autor: Propio

Con base en la implementación del Proceso de gestión de Incidentes de Ciberseguridad y la socialización con el equipo ITFIP, se debe seguir trabajando para que el proceso sea afinado y se logre dar el cumplimiento correspondiente, es

importante que se cuente con el recurso humano correspondiente para abarcar todos los frentes del proceso.

10. CONCLUSIONES

La implementación de un proceso de gestión de incidentes para el ITFIP busca estandarizar la respuesta ante cualquier incidente relacionado con los sistemas y servicios administrados por la Dirección de Tecnología, abarcando desde el registro de la ocurrencia hasta la resolución y cierre definitivo del incidente. Este proceso debe ajustarse y optimizarse continuamente para mejorar su eficiencia y obtener mejores resultados en la gestión de incidentes.

El diseño propuesto para la metodología y el plan de gestión de incidentes fortalece la capacidad de respuesta y control sobre los eventos registrados en los sistemas, permitiendo una trazabilidad precisa en la operación de servicios y sistemas, lo cual facilita la medición y evaluación de desempeño. Las métricas propuestas desempeñaron un papel clave, especialmente al no contar previamente con un sistema de medición: "lo que no se puede medir no se puede mejorar". Esta práctica ha contribuido a crear conciencia en el personal sobre la importancia de monitorear y mejorar continuamente.

Asimismo, la propuesta para la gestión de incidentes de seguridad en la infraestructura del ITFIP permite minimizar los riesgos asociados a eventos de ciberseguridad, mediante documentos de apoyo que facilitan la atención y tratamiento adecuado de estos incidentes.

Los resultados del análisis permiten confirmar que la implementación de este proceso refuerza las buenas prácticas en la gestión de incidentes de ciberseguridad, promoviendo la evolución desde un estado "Desconocido" hacia un estado "Gestionado". Este cambio representa un avance significativo, aunque se requiere continuar trabajando en la mejora continua del proceso.

La capacitación del personal en tecnología y cultura cibernética, alineada con la política institucional del ITFIP en gestión de incidentes, es fundamental para que las buenas prácticas se adopten de forma efectiva. Esto permitirá a los colaboradores responder de manera rápida, oportuna y precisa ante un incidente real de seguridad.

Finalmente, el análisis de resultados permitió determinar el estado de madurez alcanzado por el ITFIP tras la implementación del proceso de gestión de incidentes de ciberseguridad. La comparación entre el diagnóstico inicial y la evaluación posterior evidenció una mejora del **63 %** en los aspectos evaluados, lo que demuestra la efectividad de la propuesta desarrollada y su contribución al fortalecimiento de las capacidades institucionales para la gestión de incidentes.

11. LECCIONES APRENDIDAS

- Aunque las entidades pertenezcan al mismo sector o desarrollen actividades similares, cada una posee características particulares en su estructura organizacional, modelo operativo, cultura institucional y esquema de gobierno. Por esta razón, el proceso definido de gestión de incidentes de Ciberseguridad debe diseñarse y adaptarse considerando las necesidades específicas, los objetivos estratégicos o de negocio, según el contexto operativo de cada entidad pública.
- La estructura propuesta para el proceso de gestión de incidentes permite mostrar un alto nivel de adaptabilidad y puede ser implementada en diferentes entidades del sector público Colombiano, dado que se fundamenta en los lineamientos establecidos por la guía de gestión de incidentes del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), marco de referencia que orienta a las instituciones públicas del país.
- El análisis de brechas (GAP Assessment) definido en este proyecto permite evaluar el estado actual de la organización constituye una herramienta de diagnóstico que puede ser aplicable en diversos contextos institucionales. Su utilización permite establecer una línea base objetiva, identificar oportunidades de mejora, para determinar el nivel de madurez inicial antes y después del proceso de implementación.
- La mejora continua y la transferencia de conocimiento son de los temas principales que se identificaron, para garantizar la sostenibilidad del proceso de gestión de incidentes de Ciberseguridad. Estas prácticas favorecen la apropiación del proceso, fortalecen las diferentes capacidades de los equipos involucrados y contribuyen a la evolución

constante de las buenas prácticas, frente a los cambios tecnológicos, organizacionales y regulatorios.

- Los entregables definidos como parte de la documentación del proceso, incluyendo indicadores, formatos, guías de actuación, procedimientos y perfiles de roles sugeridos, deben considerarse como elementos dinámicos que pueden ser sujetos a revisión y actualización permanente. La actualización debe estar alineada con el crecimiento del área para determinar el nivel de madurez del proceso, las lecciones aprendidas deben documentarse en bases de conocimiento, obtenidas durante la operación y las necesidades que se puedan presentar en el día a día.
- La definición de roles, responsabilidades y mecanismos de coordinación entre las áreas involucradas constituye un factor clave para la efectividad en la gestión de incidentes. La articulación adecuada entre los equipos técnicos, operativos y directivos permite optimizar los tiempos de respuesta y mejorar la toma de decisiones durante situaciones de crisis.

12. TRABAJO FUTURO

Se propone un monitoreo, seguimiento o auditoria respecto a validar a la ejecución del diseño propuesto de la gestión de incidentes de ciberseguridad basado en los lineamientos de la ISO 27035 y NIST SP 800-61 y de la guía de la MINTIC. Este proyecto de grado busca contribuir a la alineación entre la estrategia corporativa de la ITFIP y los procesos de transformación digital, promoviendo una gestión oportuna frente a la atención de incidentes de ciberseguridad y una mayor resiliencia operacional. Respecto a los resultados obtenidos permitirá validar las recomendaciones derivadas de la investigación, identificar oportunidades de mejora y generar lecciones aprendidas para toma de decisiones futuras.

Definir indicadores adicionales que permitan fortalecer el proceso de gestión de incidentes de ciberseguridad, permitiendo medir del desempeño que complementen el modelo de acuerdo con las necesidades de la institución.

Ejecutar auditorias al proceso por medio de entes externos que ayuden a identificar oportunidades de mejora, para fortalecer los procesos permitiendo ser eficientes con base en las buenas prácticas, según los marcos técnicos como la NIST, las ISO y el CIS.

Finalmente, se espera que esta iniciativa sirva como referencia para futuras investigaciones relacionadas con la madurez de las capacidades de respuesta a incidentes, la automatización de procesos mediante plataformas de detección y respuesta, la integración con Centros de Operaciones de Seguridad (SOC) y la adopción de modelos avanzados de Ciber resiliencia en entornos educativos.

13. AGRADECIMIENTOS

Expresamos agradecimiento al director Alvaro Escobar, al Ing. Franchesco Mora y a los evaluadores de este proyecto de grado por su valioso acompañamiento, disposición y compromiso durante el desarrollo del proyecto. Sus recomendaciones, observaciones y correcciones fueron fundamentales para fortalecer la calidad técnica y académica del trabajo, permitiendo enriquecer el análisis, mejorar la metodología aplicada y consolidar los resultados obtenidos.

De igual manera, agradecemos la generosidad al compartir sus conocimientos y experiencia profesional, así como la orientación brindada en cada etapa del proyecto, lo que contribuyó significativamente al crecimiento académico y profesional. Su apoyo constante y dedicación fueron determinantes para culminar satisfactoriamente esta investigación, dejando importantes aprendizajes que servirán como base para futuros retos en el campo de la ciberseguridad.

14. BIBLIOGRAFÍAS

Referencias

- ANSI. (2023). ISO/IEC 27035-2: Tecnología de la información — Técnicas de seguridad — Gestión de incidentes de seguridad de la información — Parte 2: Directrices para planificar y preparar la respuesta a incidentes.
- ANSI. (2023). ISO/IEC 27035-1:2023—Tecnología de la información – Gestión de incidentes de seguridad de la información – Parte 1: Principios y proceso.
- Center for Internet Security. (05 de 2021). Controles CIS Versión 8.
- Centro Criptológico Nacional. (04 de 2020). Guía de Seguridad de las TIC - CCN-STIC817 -Esquema Nacional de Seguridad Gestión de ciberincidentes.
- COLCERT. (31 de 05 de 2023). *COLCERT*. Obtenido de COLCERT- AL-0531- 0021:
https://colcert.gov.co/800/articles-276383_Documento_1.pdf
- Departamento Administrativo de la Función Pública. (09 de 2022). *Funcion Publica*. Obtenido de <https://www.funcionpublica.gov.co>:
https://www.funcionpublica.gov.co/documents/34645357/34703120/Politica_tratamiento_datos_personales.pdf/b697c1b1-e899-4149-9415-eb810cb13ca?t=1537181695604
- Fortinet. (27 de 10 de 2021). *Fortinet*. Obtenido de
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_1500D.pdf

Fortinet. (19 de 09 de 2023). *Fortinet*. Obtenido de

<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC.pdf>

Fortinet. (3 de 11 de 2023). *Fortinet*. Obtenido de

<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf>

Fortinet. (01 de 02 de 2023). *Fortinet*. Obtenido de

<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiWeb.pdf>

Fortinet. (30 de 08 de 2023). *Fortinet*. Obtenido de

<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf>

Fortinet. (12 de 07 de 2023). *Fortinet*. Obtenido de

<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSIEM.pdf>

Fortinet. (28 de 07 de 2023). *Fortinet*. Obtenido de

<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiap-u-series.pdf>

Fortinet. (25 de 07 de 2023). *Fortinet*. Obtenido de

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSwitch_Secure_Access_Series.pdf

Hernández Sampieri, R., Fernández Collado, C., & Batista Lucio, M. (2014).

Metodología de la investigación Edi 6. Mexico: McGrawHill Education.

INCONTEC. (2013). *ISO 27001:2013 Sistema de Gestión de Seguridad de la*

Información. INCONTEC.

- ISACA. (1 de 9 de 2015). *ISACA*. Obtenido de <https://www.isaca.org/resources/isaca-journal/issues/2015/volume-5/addressing-cybersecurity-vulnerabilities>
- ISO.ORG. (2023). Information technology —Information security incident management. Suiza.
- ISO/IEC. (2022). 27005: INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECCION- GUIDANCE ON MANAGING INFORMATION SECURITY RISKS. GINEBRA, SUIZA.
- ISO/IEC 27000. (2018). 27000:2018 Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de seguridad de la información — Descripción general y vocabulario.
- Ministerio de Educación. (s.f.). *Mineduccion*. Obtenido de https://www.mineduccion.gov.co/1759/articles-398739_Guia_007.pdf
- MINTIC. (2016). *MinTIC*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf
- MinTIC. (06 de 2021). *Gobierno Digital*
- MITRE. (02 de 008 de 2023). *MITRE | ATT&CK*. Obtenido de <https://attack.mitre.org>
- NIST. (10 de 2003). *NIST*. Obtenido de <https://doi.org/10.6028/NIST.SP.800-50>
- NIST. (2020). *NIST*. Obtenido de NVLPUBS.NIST.GOV:
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- NIST. (2023). *nist*. Obtenido de CRCS.nist.gov:
<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>

Organización Internacional de Normalización (ISO. (05 de 06 de 2024). ISO 9001:2015

Sistemas de gestión de la calidad -Requisitos. Ginebra, Suiza.

Reservado. (s.f.). Obtenido de [https://www.mintic.gov.co/gestionti/615/w3-](https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6314.html?_noredirect=1)

[propertyvalue-6314.html?_noredirect=1](https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6314.html?_noredirect=1)

Reservado. (2010). *Colaboracion DNP*. Obtenido de Departamento Nacional de

Planeación: <https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3670.pdf>

Reservado. (2018). *Colaboración DNP*. Obtenido de Distrito Nacional de Planeación:

<https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3920.pdf>

Reservado. (2018). *Función publica*. Obtenido de

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=86902>

Reservado. (10 de 2023). *Secretaria del Senado*. Obtenido de

http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Reservado. (2023). *Secretaria del Senado*. Obtenido de

http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Reservado. (2023). *Secretaria Senado*. Obtenido de

http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Tejada, E. C. (2023). *Gestión de incidentes de seguridad informática*. IFCT0109. IC

Editorial.

ANEXO A¹⁵

14.1. GAP

Tabla 18 GAP

Ítem	Norma / Marco Ref	Descripción	Estado	Observación	% Cumplimiento Previo	% Cumplimiento Después de Implementación
1	ALTA DIRECCIÓN					
1,1	27001:2022	¿Existe un comité de seguridad y ciberseguridad con la alta dirección / comité académico? (Para la toma de decisiones)	Limitado	Se cuenta con un comité general en donde hay un espacio para tratar los temas de tecnología y dentro de este se habla sobre seguridad.	30%	50%
1,2	27001:2022	¿Existen directrices o procedimientos generales para la gestión de incidentes de seguridad de la información y ciberseguridad en el ITFIP?	Inexistente	No existe documentación relacionada.	0%	40%
2	PRESENTACIÓN DE INFORMES / INDICADORES					

¹⁵ Autores y equipo ITFIP

2,2	27001:2022	¿Existe un indicador para el reporte de incidentes de seguridad y ciberseguridad?	Inicial	No se cuenta con esta documentación.	5%	90%
2,3	27001:2022	¿Existen informes periódicos que permita identificar la cantidad de incidentes y eventos reportados?	Inexistente	No se cuenta con esta documentación.	0%	80%
3	PROCEDIMIENTO DE GESTION DE INCIDENTES					
3,1	ISO 27001:2022	¿Se cuenta con un planeamiento y preparación de la gestión de incidentes de seguridad de la información?	? Desconocido	No se tiene aplicado	0%	80%
3,2	NIST	¿Existe un proceso formalizado para la detección, análisis, contención, erradicación y recuperación de incidentes de seguridad de la información?	? Desconocido	No se ha contemplado	0%	80%

3,3	NIST/27035:2022/MinTIC	¿La institución cuenta con procedimientos documentados para la notificación y comunicación de incidentes dentro y fuera de la institución?	? Desconocido	No se ha contemplado	0%	80%
3,4	27035:2022/MinTIC	¿La Institución cuenta con procedimientos documentados para la detección, análisis, contención, erradicación, recuperación y lecciones aprendidas de los incidentes?	? Desconocido	No se ha contemplado	0%	80%
3,5	27035:2023/CIS V8/MinTIC	¿La Institución tiene un proceso formalizado para la gestión de incidentes de seguridad de la información?	? Desconocido	No se ha contemplado	0%	80%
4	POLÍTICAS					
4,1	ISO 27001:2022	¿Se cuenta con una Política de seguridad de la información y Ciberseguridad?	? Desconocido	No se ha contemplado	0%	80%

4,2	ISO 27001:2022	¿Se cuenta con una Política general para la gestión de incidentes de seguridad y Ciberseguridad?	Desconocido	No se ha contemplado	0%	80%
5 REQUISITOS DE FORMACIÓN, EDUCACIÓN Y SENSIBILIZACIÓN						
5,1	ISO 27001:2022	¿Se cuenta con Capacitaciones para el aprendizaje sobre los incidentes de seguridad y Ciberseguridad ?	Inexistente	No se ha contemplado	0%	80%
5,2	MinTIC	¿Se llevan a cabo actividades de sensibilización y capacitación del personal sobre la gestión de incidentes según lo sugerido en la Guía del MinTIC?	Inicial	Se realizan campañas de phishing 1 vez al año, pero no se mencionan temas de Gestión de Incidentes.	15%	80%
5,3	Propio	¿Hay un procedimiento de aprendizaje, teniendo en cuenta los incidentes de seguridad de la información y Ciberseguridad?	Inexistente	No se ha contemplado	0%	60%

5,4	Propio	¿Se generan campañas de seguridad por mails, wallpapers, comunicados etc, sobre como reportar un incidente de seguridad ?	Inicial	Se realizan campañas de phishing 1 vez al año, pero no se mencionan temas de Gestión de Incidentes.	15%	80%
6	PROCEDIMIENTOS Y MANUALES DE RESPUESTA EN EL MANEJO DE INCIDENTES					
6,1	ISO 27001:2022	¿ Se cuenta con un procedimiento de respuesta a los incidentes de seguridad y ciberseguridad?	Inexistente	No se ha contemplado	0%	80%
6,2	ISO 27001:2022	¿Se tiene definido un procedimiento para la recolección de evidencia?	Inexistente	No se ha contemplado	0%	80%
6,3	NIST	¿Se mantiene un registro de incidentes históricos y se utilizan para informar sobre las tendencias y patrones de ataques?	Inexistente	No se ha contemplado	0%	80%

6,4	27035:2023	¿Se realizan evaluaciones regulares de riesgos para identificar posibles amenazas y vulnerabilidades que puedan dar lugar a incidentes de seguridad de la información?	Inexistente	No se ha contemplado	0%	80%
6,5	27035:2024	¿La Institución tiene protocolos establecidos para la recopilación y preservación de evidencia forense durante la investigación de incidentes?	Inexistente	No se ha contemplado	0%	20%
7	COMUNICACIÓN INTERNA Y EXTERNA					
7,1	CIS V8	¿Se tiene establecido un proceso institucional para informar un incidente?	Inexistente	No se ha contemplado	0%	80%
7,2	ISO 27001:2022	¿Se tiene definido el reporte de eventos de seguridad y ciberseguridad?	Inexistente	No se ha contemplado	0%	80%

7,3	27035:2023	¿Se ha establecido un proceso claro de comunicación interna y externa durante la gestión de incidentes? (Matriz de escalamiento)	Inexistente	No se ha contemplado	0%	80%
7,4	MinTIC	¿La Institución cuenta con mecanismos de reporte y notificación de incidentes establecidos, en línea con las recomendaciones de la Guía del MinTIC?	Inexistente	No se ha contemplado	0%	60%
7,5	MinTIC	¿Se han definido protocolos de comunicación interna y externa durante la gestión de incidentes, siguiendo las pautas proporcionadas por el MinTIC?	Inexistente	No se ha contemplado	0%	60%
7,6	CIS V8	Definir mecanismos de comunicación durante la respuesta a incidentes	Inexistente	No se ha contemplado	0%	60%
8	EVALUACIÓN Y MEJORA CONTINUA					

8,1	ISO 27001:2022	¿Se hace evaluación para toma de decisión en los eventos de seguridad de la información?	Inexistente	No se ha contemplado	0%	40%
8,2	27035:2023/ NIST / CISV8	¿Se llevan a cabo ejercicios de simulación y pruebas para evaluar la efectividad del proceso de gestión de incidentes?	Inexistente	No se ha contemplado	0%	10%
8,3	NIST 27035:2027	¿La Institución tiene un plan de mejora continua para fortalecer su capacidad de gestión de incidentes según los requisitos de la NIST 800-61 Rev. 2 /ISO 27035:2023?	Inexistente	No se ha contemplado	0%	40%
8,4	27035:2026 Mintic	¿Se documentan adecuadamente todos los incidentes, acciones tomadas y lecciones aprendidas para su análisis posterior y mejora continua?	Inexistente	No se ha contemplado	0%	40%

8,5	27035:2023/ Mintic/27001: 2022	¿Existe un compromiso continuo de mejora basado en las recomendaciones y buenas prácticas proporcionadas por marcos de referencia en Gestión de Incidentes?	Inexistente	No se ha contemplado	0%	40%
8,6	CIS V8	¿Se realizan revisiones posteriores a un incidente?	Inexistente	No se ha contemplado	0%	20%
8,7	CIS V8	¿Se establecen y mantienen umbrales de incidentes de seguridad?	Inexistente	No se ha contemplado	0%	40%
9	ROLES Y RESPONSABILIDADES					
9,1	NIST 27035:2023	¿La Institución tiene un equipo de respuesta a incidentes (IRT) designado y capacitado para manejar los incidentes de seguridad y Ciberseguridad?	Inexistente	No se ha contemplado	0%	60%

9,2	NIST 27035:2023 MinTIC CIS V8	¿Se han asignado o definido roles y responsabilidades claves para los miembros del equipo de respuesta a incidentes?	Inexistente	No se ha contemplado	0%	40%
9,3	CIS V8	¿Se tiene designado personal para administrar el manejo de incidentes?	Inexistente	No se ha contemplado	0%	30%
9,4	CIS V8	¿Se tiene establecido datos de contacto para informar incidentes de seguridad?	Inexistente	No se ha contemplado	0%	80%
9,5	NIST	¿Se realizan evaluaciones periódicas de riesgos para identificar posibles amenazas y vulnerabilidades que puedan dar lugar a incidentes de seguridad de la información?	Inexistente	No se ha contemplado	0%	40%
9,6	Propio	¿Existe una definición de responsabilidades y procedimientos para los diferentes tipos de incidentes?	Inexistente	No se ha contemplado	0%	80%

9,7	MinTIC	¿La Institución cuenta con herramientas y recursos adecuados para llevar a cabo las actividades de gestión de incidentes de acuerdo con las recomendaciones de la Guía del MinTIC?	Inexistente	No se ha contemplado	0%	60%
-----	--------	--	-------------	----------------------	----	-----

ANEXO B¹⁶

14.2. Check de Incidentes

Tabla 19 Lista de Chequeo

Lista de Chequeo para el manejo de incidentes en ciberseguridad	
Antes	
1	Realizar una evaluación de riesgos de incidentes en ciberseguridad
2	Definir y clasificar los tipos de incidentes de seguridad
3	Tener un inventario de la información y los recursos más importantes para la operación, de acuerdo con la evaluación de riesgos.

¹⁶ Autores basados en la NIST 800-61

4	De acuerdo con el anterior numeral, se tienen identificados los responsables de administrar la información y los recursos.
5	Tener definidos los responsables de gestionar la crisis, en el área legal, de comunicaciones, operaciones y recursos humanos, entre otros.
6	Documentar los roles y responsabilidades de cada cargo clave responsable de gestionar la crisis
7	Establecer los umbrales que maneja cada incidente de acuerdo con la calificación de su nivel de riesgo
8	Tener una base de datos actualizada, con diferentes números alternos de contacto de los miembros responsables de gestionar la crisis.
9	Verificar que la organización cuenta con los controles de monitoreo necesarios para proteger y mitigar cualquier fuga de información (antivirus, cortafuegos)
10	Tener un flujograma de la información que permita identificar los niveles de autoridad para la toma de decisiones ante una crisis.
11	Capacitar a los colaboradores en la administración y seguridad de la información tanto desde la perspectiva tecnológica como ética.
12	Preparar a los colaboradores, proveedores y clientes en la identificación y denuncia de acciones sospechas con la información de la organización, así como frente a incumplimientos identificados y niveles de responsabilidad desde cada rol.
13	Proyectar comunicados de prensa que describan cómo y con quién se está resolviendo el incidente, así como las acciones correctivas frente a la causa raíz.

Durante	
14	Tener un base que permita consolidar todos los incidentes reportados
15	Convocar al equipo responsable de atender y/o gestionar los incidentes para tomar las acciones necesarias para restaurar las operaciones.
16	Convocar una teleconferencia con las partes interesadas para informar oficialmente sobre la situación presentada y las acciones a seguir.
17	Identificar la causa inicial del incidente y solicitar el apoyo de los especialistas
18	Realizar una valoración de la situación presentada, el origen y los posibles planes de acción a seguir
19	En caso de identificar los equipos desde donde se presentó el incidente, mantenerlos bajo custodia para proceder con los especialistas en el desarrollo de copias y correspondiente custodia.
20	Entregar y/o conservar en custodia todos los elementos que sirven como evidencia para iniciar los procesos legales que correspondan.
21	Realizar una reunión y/o teleconferencia con los miembros de la Junta Directiva de la organización, para reportar el estado de la situación.
22	Documentar el incidente y realizar un informe sobre el mismo
23	Convocar a los especialistas para iniciar el proceso de restauración.
24	Activar el protocolo de comunicación tanto a nivel interno como externo (medios de comunicación), así como frente a los entes de control que aplique.
25	Comunicarse con los terceros afectados

Después	
26	Actualizar el informe inicialmente emitido, detallando la información sobre la situación que se presentó, en dónde se presentó y cuándo se presentó.
27	Validar si se cumplieron con las acciones esperadas durante el incidente, tanto por el personal responsable de gestionar la crisis, como por la administración.
28	Confirmar si se siguieron los procedimientos y/o protocolos establecidos.
29	Revisar si se deben realizar cambios en los controles de IT, para prevenir nuevos incidentes iguales, o no identificados al inicialmente presentado.
30	Identificar cuál fue la información y/o control que no se identificó oportunamente para prevenir dicha situación.
31	Determinar que herramientas o recursos adicionales se requieren en la organización para detectar, clasificar, analizar y mitigar futuros incidentes.
32	Revisar cuales son las normas e informes que se deben implementar a futuro para prevenir los incidentes.
33	Validar si las nuevas acciones van a mitigar dichas situaciones a futuro.
34	Cuantificar el costo económico, reputacional y operativo del incidente.
35	Emitir el correspondiente informe final a los entes internos y/o externos que corresponda.

Autor: Propio basado a la guía de la NIST SP.800-61r2 Computer Security Incident

Handling (NIST, 2020)

14.3. Formato para reporte de Incidentes de Ciberseguridad

ID del incidente:							
Fecha y hora de notificación del incidente:							
PERSONA QUE REPORTA							
Nombre:							
Perfil:	Administrativo		Estudiante		Otro		¿Cual?:
Cargo:							
Dependencia:							
Correo electrónico:					Teléfono de contacto:		
DATOS DEL INCIDENTE							
Fecha y hora de inicio del incidente:							
Medio de reporte (llamada, correo, verbal):							
CLASIFICACIÓN							
Impacto en la confidencialidad o privacidad de la información		Acceso no autorizado a recursos de información o datos sensibles (lógico o físico)					

	Hurto, fraude o pérdida de información	Uso indebido de recursos de información (físicos o tecnológicos)
	Indisponibilidad de activos de información	Suplantación de identidad
	Modificación o destrucción no autorizada de información	Divulgación no autorizada de información
	Fallas o vulnerabilidades de software o infraestructura tecnológica	Ataque informático o infección de código malicioso (propagación de virus)
	¿Otro?	
DESCRIPCIÓN DETALLADA DEL INCIDENTE		
¿Qué ocurrió?		
¿Cómo ocurrió?		
¿Porque ocurrió?		
OTRAS FUENTES DE INFORMACIÓN		
Contactos de personas que pueden ampliar información acerca del incidente		
Nombres y apellidos / Correo electrónico / Número telefónico de contacto:		
•		

Evaluación del evento.

Activos de información involucrados	
-------------------------------------	--

CRITICIDAD DEL EVENTO			
	Inferior – Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas		
	Bajo – Sistemas que apoyan a una sola dependencia o proceso de una entidad.		
	Medio – Sistemas que apoyan más de una dependencias o proceso de la entidad		
	Alto – Sistemas que apoyan procesos importantes y estaciones de trabajo de usuarios con funciones críticas		
	Superior – Sistemas de operación transaccional crítica y de información altamente sensible		
ANALISIS DEL INCIDENTE			
Fecha de inicio de investigación:			
Fecha fin de la investigación:			
Nombre y apellido de quien investiga:			
Cargo de quien investiga el incidente:		Dependencia de quien investiga:	
Evidencia recolectada para el análisis			
Actividades realizadas para el análisis			

Vulnerabilidades detectadas ¿Por qué ocurrió?				
¿Es un incidente de seguridad y privacidad de la información?	SI		NO	
Observaciones				
NOTIFICACIÓN DEL INCIDENTE				
Consejo superior	Rectoría	Vicerrectoría Académica	Vicerrectoría Administrativa	
Dirección Financiera	Departamento jurídico	Recursos Humanos	Otros departamentos	
Entidades externas (¿Cuáles?)				
Observaciones asociadas a la notificación del incidente				

Acciones planificadas

--

Lecciones aprendidas

--

14.4. Formato de resolución rápida para incidentes de Ciberseguridad

ID del incidente:							
Fecha y hora de detección:							
Identificación del Incidente							
Origen del reporte: (Usuario, SOC, Herramienta de monitoreo)							
Prioridad:	Critico		Alto		Medio		Bajo:
Descripción del incidente: (Tipo de ataque, afectación, sistema impactado)							
Contención Inicial							
Aislar sistemas afectados (Desconexión de la red)							
Bloqueo de IoC – IPs, dominios (Firewall, IDS, Proxy,)							
Cambiar credenciales comprometidas (si hay indicios de robo)							

Guardar evidencias (Logs, capturas, archivos sospechosos)	
Análisis y Diagnostico	
Herramientas de análisis: (Antivirus, SIEM, escáner de vulnerabilidades)	
Evaluar el alcance: (Usuarios, dispositivos, datos comprometidos)	
Identificar vector de ataque: (Phishing, exploit, RDP abierto, etc.)	
Erradicación	
Eliminar archivos maliciosos o procesos sospechosos:	
Aplicar parches o actualizaciones necesarias	

Revisar configuraciones de seguridad: (Endpoints, servidores, aplicaciones)	
Recuperación	
Restaurar sistemas desde copias de seguridad confiables	
Reintegrar los sistemas a la red: (Es necesario estar seguros)	
Monitorear actividad post-incidente: (Para detectar anomalías)	
Lecciones aprendidas	
Reunión post-incidente: (Análisis detallado con todas las partes)	
Actualizar políticas de seguridad: (Según los hallazgos)	

Capacitación al personal: (Para evitar incidentes similares)	
Documentación Final	
Resumen del incidente	
Medidas correctivas implementadas	
Recomendaciones futuras	

14.5. Formato Verificador de servicios post-Incidente de Ciberseguridad

Fecha: _____

Hora de verificación: _____

Nombre del verificador: _____

Nombre del incidente: _____

Fecha/hora de resolución del incidente: _____

1. Verificación de Sistemas Críticos

Sistema / Servicio	Estado	Observaciones	
--------------------	--------	---------------	--

Servidor de autenticación (AD, LDAP)	☐ OK ☐ Falla		
Servicios de red (DNS, DHCP, VPN)	☐ OK ☐ Falla		
Correo electrónico empresarial	☐ OK ☐ Falla		
Sistemas operativos de servidores	☐ OK ☐ Falla		
Firewall y dispositivos perimetrales	☐ OK ☐ Falla		
Plataforma de monitoreo (SIEM, logs)	☐ OK ☐ Falla		
Aplicaciones críticas de negocio	☐ OK ☐ Falla		
Base de datos principal	☐ OK ☐ Falla		
Backups y restauración	☐ OK ☐ Falla		

2. Verificación de Seguridad.

Actividad / Control	Realizado	Detalles
Aplicación de parches / actualizaciones	☐ Sí ☐ No	

Escaneo de malware / antivirus completo	☐ Sí ☐ No	
Revisión de logs por actividad anómala	☐ Sí ☐ No	
Cambio de contraseñas comprometidas	☐ Sí ☐ No	
Validación de integridad de archivos	☐ Sí ☐ No	
Verificación de cuentas de usuarios	☐ Sí ☐ No	
Revisión de accesos remotos habilitados	☐ Sí ☐ No	

3. Comunicación y documentación

Tarea	Realizado	Responsable
Notificación a usuarios o áreas afectadas	☐ Sí ☐ No	
Actualización del ticket o registro del incidente	☐ Sí ☐ No	
Documentación de acciones correctivas	☐ Sí ☐ No	

Revisión de políticas afectadas	☐ Sí ☐ No	
------------------------------------	---	--

4. Observaciones adicionales.

5. Firma Validación.

Verificador de sistemas _____ (Firma)

Responsable de Ciberseguridad _____ (Firma)

14.6. Bitácora de Incidentes de Ciberseguridad

Nombre de la organización: ITFIP

Responsable del registro: _____

Fecha de inicio del registro: ____ / ____ / ____

Última actualización: ____ / ____ / ____

Registro de incidentes

ID	1	2
Fecha y Hora del Incidente	XXX	XXX
Tipo de Incidente	Phishing	Malware
Descripción del Incidente	Correo sospechoso recibido por varios usuarios.	Activación de archivo adjunto malicioso en estación de trabajo.
Sistemas Afectados	Correo corporativo	Equipo del usuario, red interna
Usuario(s) Involucrado(s)		
Acción Inmediata Tomada	Correo bloqueado	Desconexión de la red, escaneo con antivirus
Análisis Causa Raíz	Usuario hizo clic en enlace malicioso	Ingeniería social, correo falso
Acciones Correctivas / Preventivas	Capacitación, reglas de filtrado mejoradas	Revisión de políticas de adjuntos, actualización de AV
Estado	Cerrado	Cerrado
Responsable del Seguimiento		

Notas Adicionales / Observaciones generales

Recomendaciones de uso:

- Mantener actualizado después de cada incidente.
- Guardar versiones controladas (ej. con número de versión y fecha).
- Revisar regularmente para análisis de tendencias y mejora continua.

14.7. Formato de Comunicación de Incidentes de Ciberseguridad.
Datos Generales del Incidente

ID del incidente:	
Fecha y hora de detección:	
Origen del Incidente: [Interno / Externo / Usuario / Proveedor / Automatización / Otro]	

Clasificación del Incidente: [Acceso no autorizado / Malware / Phishing / Fuga de información / Denegación de servicio / Otro]						
Severidad:	Alta		Media		Baja	
Descripción Breve del Incidente:						
Responsables y escalamientos						
Rol	Responsable	Medio de Contacto			Tiempo de Respuesta Esperado	
Primer Respondedor (TI / SOC)	Nombre	[Email / Teléfono / Chat]			Inmediato (0-15 min)	

Encargado del Servicio / Proceso Afectado	Nombre	[Email / Teléfono / Chat]	< 30 min
CISO / Responsable de Seguridad	Nombre	[Email / Teléfono / Chat]	< 1 hora
Alta Dirección / Comité de Crisis (si aplica)	Nombre	[Email / Teléfono / Chat]	Según evaluación
Criterios para escalamiento: (El incidente debe ser escalado si cumple al menos uno de los siguientes criterios)			
Afecta servicios críticos o disponibilidad de sistemas esenciales.			
Implica pérdida o compromiso de datos personales o confidenciales.			

Tiene impacto externo (clientes, proveedores, usuarios finales)			
Requiere intervención legal o notificación a entes regulatorios			
No se puede contener con los recursos iniciales			
Comunicación (Una vez validado el incidente, se informará a los siguientes grupos según su relación con el evento)			
Parte interesada	Medio de Comunicación	Responsable	Tiempo de Notificación
Dueños del proceso / servicio	Correo / Reunión urgente/chat	TI / Seguridad	< 30 min desde validación
Usuarios internos	Correo / Reunión urgente/chat	Comunicaciones / TI	Según impacto

Clientes afectados	Correo / Reunión urgente/chat	Soporte al cliente / Legal	< 4 horas si aplica
Proveedores involucrados	Correo / Reunión urgente/chat	TI / Compras / Legal	< 4 horas si aplica

Formato de Notificación (Plantilla Breve para Comunicación)

Asunto: Notificación de Incidente de Ciberseguridad [ID] – [Clasificación]

Estimado/a [Nombre o Grupo],

Se ha detectado un incidente de ciberseguridad clasificado como [Clasificación], ocurrido el día [Fecha] a las [Hora].

El incidente afecta al proceso/servicio: [Nombre del proceso o sistema], y se encuentra en fase de [Contención / Investigación / Resolución].

Impacto estimado: [Resumen del impacto].

Estamos trabajando activamente para mitigar la situación. Proporcionaremos actualizaciones conforme avance la resolución.

Si tiene dudas o requiere más información, comuníquese con [Nombre y contacto del responsable].

Atentamente,

[Nombre del Equipo de Seguridad o CISO]

[Contacto]

14.8. Formato Matriz de Contactos de emergencia

Información General

Documento: Matriz de Contactos de Emergencia

- Versión: 1.0

- Fecha de Actualización: [_____/_____/_____]

- Responsable de Actualización: [Nombre / Puesto]

1. Instrucciones de Uso.

- Esta matriz debe mantenerse actualizada en todo momento.
- Ante un incidente, contactar primero a los responsables primarios; si no hay respuesta, escalar a los contactos secundarios.
- Toda acción y comunicación deben ser registradas en los reportes de incidentes correspondientes.
- Actualización periódica: Al menos una vez cada 6 meses o tras cualquier cambio relevante en personal o proveedores.

2. Tabla de Contactos

Categoría	Nombre	Puesto / Rol	Empresa	Correo	Teléfono	Horario de Disponibilidad	Nivel de escalamiento (1,2,3)
Equipo de Respuesta a Incidentes (CSIRT)	Wilson Mauricio Pimiento Cardénas (E)	Líder de CSIRT	ITFIP	wpimiento@itfip.edu.co	3133524512	24/7	1
Equipo de respuesta a incidentes (CSIRT)	NO asignado	Analista forense	Contratista	N/A	N/A	8*5	2
Especialistas Externos	NO asignado	Consultor Forense	Proveedor	N/A	N/A	ANS	2
Especialistas Legales	Amparo Sánchez Perdomo	Asesor Legal en Ciberseguridad	ITFIP	Asanchez560@itfip.edu.co	N/A	24/7	1
Comunicaciones	Diana Delgado	Encargado de Comunicación de Crisis	ITFIP	bienestar@itfip.edu.co	N/A	24/7	2

TI Infraestructura	Wilson Mauricio Pimiento Cardénas	Responsable de Redes	ITFIP	<a href="mailto:wpimient
o@itfip.e
du.co">wpimient o@itfip.e du.co		24/7	1
Autoridades / Reguladores	N/A	Enlace con ColCERT Nacional	ColCER T	<a href="mailto:contact
o@colc
ert.gov.
co">contact o@colc ert.gov. co	N/A	24/7	3

3. Glosario de Categorías.

- CSIRT: Computer Security Incident Response Team (Equipo de Respuesta a Incidentes).
- Especialistas Externos: Expertos forenses, recuperación de datos, consultores de respuesta.
- Especialistas Legales: Asesoría en temas regulatorios, legales y notificación de incidentes.
- TI Infraestructura: Encargados de redes, servidores, bases de datos críticos.
- Autoridades: Enlace con ColCERT, policía cibernética, o autoridades regulatorias.

ANEXO C¹⁷

14.9. Guía escenario general

14.10. Guía casos – Respuesta a incidentes.

Procedimiento general de respuesta a incidentes	
Proceso	• Documentación completa, paso a paso de evidencias recolectadas, registros, recolección de información.
Identificar el incidente	• Análisis de la información e información recolectada para determinar si es un incidente de ciberseguridad
Notificación.	• Transmitir y notificar a los responsables que corresponde al tipo de incidente de ciberseguridad. • De acuerdo con la criticidad del incidente, notificar al ente externo ColCERT C-SIRT solicitando ayuda especializada para la gestión del incidente.
Contención – Erradicación – Mitigación	• Activar las herramientas y procedimientos necesarios para mitigar o contener los incidentes, sin alterar parte de la evidencia o el sistema afectado

¹⁷ Autores

Análisis - Investigación	• información completa o la más necesaria respecto a la evidencia levantada del incidente. • Investigación del incidente con el objetivo de buscar causa, raíz, técnicas empleadas, tareas o acciones realizadas basado en las evidencias recolectadas.
Recuperación del Incidente	• Resolución del incidente desde el origen que lo provoco. • Confirmar el estado normal de la operación de los sistemas luego de un tiempo prudencial.
Actividades Post- incidente , Lecciones aprendidas	• Documentación completa y registrada en los incidentes de ciberseguridad, documento técnico y ejecutivo. • Registrar los procesos realizados, errores cometidos en el proceso de la gestión del incidente de ciberseguridad. • Acciones de mejora al grupo de respuesta a incidentes, planes de trabajo, capacitación técnica o procedimental con el objetivo del mejoramiento a la gestión de incidentes de ciberseguridad.

Autor: Propio

14.11. Guía - Casos de Intrusión.

Procedimiento para realizar en caso de un incidente de ciberseguridad o indicio de que este ocurriendo.
1. En todo el Proceso
Registrar o documentar todo el proceso, que incluye cambios, configuraciones, evidencias recolectadas, acciones, planes de trabajo, datos entregados por usuarios y administradores que relacionan el incidente.
2. Detección -Análisis
Con la información y evidencia recolectada, conformar si se trata de un incidente de ciberseguridad
• Trafico anómalo en los sistemas (entrada, salidas) • Aplicaciones nuevas en los sistemas, servidores • Comportamiento anormal de los sistemas y aplicaciones • Logs anómalos en los sistemas afectados y dispositivos perimetrales. • Anomalías en el performance de los sistemas • Realizar una copia o imagen del sistema. • Volcado de memoria al sistema • Obtener evidencia sin alterar el sistema afectado. • Análisis de eventos en el correlacionador centralizado. SIEM

• Realizar un análisis forense del sistema, para realizar un trabajo detallado y exhaustivo. • Verifica la no existencia de compromisos en otros sistemas, movimientos laterales.
3. Notificación.
Transmitir y notificar a los responsables que corresponde al tipo de incidente de ciberseguridad. De acuerdo con la criticidad del incidente, notificar al ente externo ColCERT C-SIRT solicitando ayuda especializada para la gestión del incidente
4. Contención.
• Bloquear todo posible acceso al sistema o directamente al servidor afectado-vulnerable • Bloquear todo tipo de indicadores de compromiso: objetos, IPs, Hash, Dominios • Aislamiento de los sistemas, físico y lógico • Activar las herramientas y procedimientos necesarios para mitigar o contener los incidentes, sin alterar parte de la evidencia o el sistema afectado. • Activar herramientas de seguridad en cada uno de los controles: gestión de acceso etc.
5. Erradicación y recuperación.

- Apagado del sistema después de realizado una copia o volcado de memoria y que no sea crítico para la organización.
- Sanitizado del sistema, limpieza total y profunda de libre de código malicioso, anomalías, indicadores de compromiso y cualquier componente externo del mismo sistema.
- En caso de que el sistema fue comprometido, realizar la última restauración o copia del sistema limpio.
- Reinstalación del sistema operativo, aplicaciones.
- Parchado y corrección de vulnerabilidades en los sistemas.
- Verificación del estado de salud de los sistemas estén en condiciones normales.
- Contactar y aplicar recomendaciones del agente externo respecto a tratamiento de incidentes de ciberseguridad ColCERT

6. Actividades Post incidente-Lecciones Aprendidas

- Documentación completa y registrada en los incidentes de ciberseguridad, documento técnico y ejecutivo.
- Registrar los procesos realizados, errores cometidos en el proceso de la gestión del incidente de ciberseguridad.
- Acciones de mejora al grupo de respuesta a incidentes, planes de trabajo, capacitación técnica o procedimental con el objetivo del mejoramiento a la gestión de incidentes de ciberseguridad.

- Activar las herramientas y procedimientos necesarios para mitigar o contener los incidentes, sin alterar parte de la evidencia o el sistema afectado

Autor: Propio basado a la guía de la NIST SP.800-61r2 Computer Security Incident Handling Guide (NIST, 2020) y el centro criptológico nacional (Centro Criptológico Nacional, 2020)

14.12. Guía – Casos de Denegación de servicios.

Procedimiento para realizar en caso de un incidente de ciberseguridad o indicio de que este ocurriendo.	
0. En todo el Proceso	
Registrar o documentar todo el proceso, que incluye cambios, configuraciones, evidencias recolectadas, acciones, planes de trabajo, datos entregados por usuarios y administradores que relacionan el incidente.	
1. Detección y análisis	
Con la información y evidencia recolectada, confirmar si se trata de un incidente de ciberseguridad	
• Trafico anómalo en los sistemas (entrada, salidas) • Comportamiento anormal de los sistemas y aplicaciones, performance	

- Servicio degradado, lentitud en los sistemas, respuestas de los servicios fuera de lo normal.
- Trafico utilizado (TCP, UDP, ICMP)
- Geolocalización de los orígenes de tráfico, score alto o reputación maliciosa de los orígenes.
- Análisis de tráfico, tipos de peticiones, botnet, Host robots generadores de solicitudes.
- Investigación de los métodos de ataque y orígenes.
- Capturar un equipo del cual se realiza el ataque (botnet) y tomar la mayor parte de información y evidencia para analizar y entender los vectores de ataque para dar algún tipo de solución.
- Realizar reconocimiento de información externa en los sitios o foros de publican información respecto al origen o el tipo de ataque,

2. Notificación.

Transmitir y notificar a los responsables que corresponde al tipo de incidente de ciberseguridad.

De acuerdo con la criticidad del incidente, notificar al ente externo ColCERT C-SIRT solicitando ayuda especializada para la gestión del incidente

3. Contención.

A nivel de Red:

- Bloquear todo posible acceso al sistema o directamente al servidor o servicios afectados-vulnerables.
- Activar los sistemas de defensa perimetral, Anti-DDOS, reglas de bloqueo por spoof o inundaciones de tráfico.
- Bloqueo desde el WAF o Firewall, tráfico anómalo, orígenes de las IPS, Geo protección, ancho de banda de las interfaces.
- Balanceo de carga desde el balanceador de tráfico, (Akamai, Imperva) etc.
- Uso de redes de distribución de contenido.
- Bloqueo desde los mecanismos de Anti-spoofing, Anti-flood.
- Bloqueo a nivel de IPS en sus reglas de Anti-DDOS
- Revisión de las reglas de filtrado de contenido y control de aplicación.
- Disminución de la capacidad de ancho de banda del tráfico (entrada/salida) si se permite para no afectar sistemas críticos.
- Se puede activar la ampliación del ancho de banda si está saturado, se debe evaluar si es posible.
- Asilamiento de servicios o redes comprometidas, desconexión de redes.
- Desconexión de la Internet de los sistemas, mantener la disponibilidad de los servicios a nivel interno, este se debe evaluar el impacto si es posible.
- Activar las herramientas y procedimientos necesarios para mitigar o contener los incidentes, sin alterar parte de la evidencia o el sistema afectado.

A nivel de servidores DNS

- Cambios en el apuntamiento de los servicios de DNS, modificar en la controladora de dominio, balanceadores de carga.
- Uso de servicio de resolución de DNS registrados.
- Uso de servidores DNS ajenos, redes de confianza.

A nivel de Servidores de Correo.

- Uso de listas blancas y negras según el caso, endurecimiento del control.
- Ingreso de indicadores de compromiso – cuentas de correo tipo spam
- Activación de módulos anti-spam,

A nivel de servidores Web.

- Activar controles o mecanismos de bloqueo en la capa de aplicación plugins respecto a excesos de peticiones y consultas.
- Bloqueo a nivel de firewall de aplicación- WAF , tráfico malicioso, score alto
- Inactivar módulos o capas de los sitios web, obteniendo aceleraciones de las páginas web y capacidad de respuesta.

• Uso de plantillas o paginas ligeras, uso de recursos necesarios.
4. Erradicación y recuperación.
• Verificación del estado de salud de los sistemas estén en condiciones normales. • Apoyo de los equipos de respuesta a incidentes y el ISP para activación de control de tráfico. • Desactivación de redes maliciosas, botnets. • Filtrado de tráfico y contenido desde el ISP • Contactar y aplicar recomendaciones del agente externo respecto a tratamiento de incidentes de ciberseguridad ColCERT
5. Actividades Post incidente-Lecciones Aprendidas
• Documentación completa y registrada en los incidentes de ciberseguridad, documento técnico y ejecutivo. • Registrar los procesos realizados, errores cometidos en el proceso de la gestión del incidente de ciberseguridad. • Acciones de mejora al grupo de respuesta a incidentes, planes de trabajo, capacitación técnica o procedimental con el objetivo del mejoramiento a la gestión de incidentes de ciberseguridad. • Activar las herramientas y procedimientos necesarios para mitigar o contener los incidentes, sin alterar parte de la evidencia o el sistema afectado

Autor: Propio basado a la guía de la NIST SP.800-61r2 Computer Security Incident Handling Guide (NIST, 2020) y el centro criptológico nacional (Centro Criptológico Nacional, 2020)

14.13. Guía – Casos de Código Malicioso.

Procedimiento para realizar en caso de un incidente de ciberseguridad o indicio de que este ocurriendo.
0. En todo el Proceso
Registrar o documentar todo el proceso, que incluye cambios, configuraciones, evidencias recolectadas, acciones, planes de trabajo, datos entregados por usuarios y administradores que relacionan el incidente.
1. Detección y análisis
Con la información y evidencia recolectada, conformar si se trata de un incidente de ciberseguridad
• Trafico anómalo en los sistemas (entrada, salidas) • Aplicaciones nuevas en los sistemas, servidores • Comportamiento anormal de los sistemas y aplicaciones • Logs anómalos en los sistemas afectados (auditoria, seguridad, visor de registros) y dispositivos perimetrales. • Anomalías en el performance de los sistemas • Realizar una copia o imagen del sistema.

- Volcado de memoria al sistema
- Obtener evidencia sin alterar el sistema afectado.
- Análisis de eventos en el correlacionador centralizado. SIEM
- Realizar un análisis forense del sistema, para realizar un trabajo detallado y exhaustivo.
- Verifica la no existencia de compromisos en otros sistemas, movimientos laterales.
- Análisis del malware con herramientas licenciadas y sofisticadas para descubrir los patrones, reglas YARA, uso de Sandbox.

2. Notificación.

Transmitir y notificar a los responsables que corresponde al tipo de incidente de ciberseguridad.

De acuerdo con la criticidad del incidente, notificar al ente externo ColCERT C-SIRT solicitando ayuda especializada para la gestión del incidente

3. Contención.

- Bloquear todo posible acceso al sistema o directamente al servidor afectado vulnerable.
- Aislar los sistemas y equipos comprometidos a nivel lógico y físico
- Bloqueo de todo el malware posible en la red, sistemas de antivirus, EDR.
- Bloquear todo tipo de indicadores de compromiso: objetos, IPs, Hash, Dominios.

- Deshabilitar protocolos respecto a compartir información, ficheros , delimitar y monitorear el protocolo SMB.
- Bloqueo de los sistemas mediante dispositivos de red (router, firewalls).
- Bloqueo de tráfico, estrangulación de toda la red que sea posible.
- Bloque a nivel de consola de correo a través de modulo anti-spam, listas negras, subject del correo.
- Despliegue de antivirus en los sistemas, actualización de firmas, Antispam, Antispyware
- Bloqueo desde el IPS.
- Activar las herramientas y procedimientos necesarios para mitigar o contener los incidentes, sin alterar parte de la evidencia o el sistema afectado.
- Activar herramientas de seguridad en cada uno de los controles: gestión de acceso etc.

4. Erradicación y recuperación.

- Apagado del sistema después de realizado una copia o volcado de memoria y que no sea crítico para la organización.
- Sanitizado del sistema, limpieza total y profunda de libre de código malicioso, anomalías, indicadores de compromiso y cualquier componente externo del mismo sistema.
- En caso de que el sistema fue comprometido, realizar la última restauración o copia del sistema limpio.

- Reinstalación del sistema operativo, aplicaciones.
- Parchado y corrección de vulnerabilidades en los sistemas.
- Verificación del estado de salud de los sistemas estén en condiciones normales.
- Contactar y aplicar recomendaciones del agente externo respecto a tratamiento de incidentes de ciberseguridad ColCERT

5. Actividades Post incidente-Lecciones Aprendidas

- Documentación completa y registrada en los incidentes de ciberseguridad, documento técnico y ejecutivo.
- Registrar los procesos realizados, errores cometidos en el proceso de la gestión del incidente de ciberseguridad.
- Acciones de mejora al grupo de respuesta a incidentes, planes de trabajo, capacitación técnica o procedimental con el objetivo del mejoramiento a la gestión de incidentes de ciberseguridad.
- Activar las herramientas y procedimientos necesarios para mitigar o contener los incidentes, sin alterar parte de la evidencia o el sistema afectado

Autor: Propio basado a la guía de la NIST SP.800-61r2 Computer Security Incident Handling Guide (NIST, 2020) y el centro criptológico nacional (Centro Criptológico Nacional, 2020)

14.14. Guía – Casos identificar posible amenaza.

Procedimiento para responder a un incidente o identificar una posible amenaza	
0. Durante todo el proceso	
Documentación completa: Incluir todas las acciones realizadas, evidencia recolectada, chats, correos, conversaciones y datos suministrados por usuarios, administradores y demás personas involucradas con el incidente.	
1. Identificación del incidente	
Apoyarse con el grupo de trabajo para la documentación y revisión de los sistemas monitoreados para la búsqueda de anomalías.	
Análisis del escenario con la evidencia inicial para confirmar o descartar si se trata de un incidente.	
2. Notificación	
Iniciar la etapa de notificación involucrado a los lides y responsables de la institución. En este punto se debe ser lo más claro y tratar de omitir información sensible respecto a la fuga de información.	
Notificación a los entes nacionales como es el ColCERT - CSIRT para solicitar ayuda especializada en la gestión del incidente (si la criticidad del incidente lo requiere).	
3. Contención y mitigación del incidente	

Activar el plan de mitigación de plataforma y procesos para contener la amenaza, con esto se reduce los servicios y sistemas que puedan afectar en la operación. Aislamiento de sistemas lógicos y físicos.
4. Análisis e Investigación
Evidencias completas de los sistemas que sustente el incidente de seguridad.
Almacenar toda la descripción y documentación detallada de cada evidencia recogida.
Análisis de las evidencias buscando patrones de indicadores de compromiso que incluye: origen, protocolos, servicios, técnicas de ataque empeladas, acciones y demás información necesaria.
5. Solución y Recuperación
Resolución del incidente basándose en la mitigación o contención del origen respectivo de la amenaza
Luego de lograr contener y dar solución al incidente, dar un tiempo prudencial para la estabilización del sistema antes de notificar con normalidad de los sistemas.
En caso de detectarse actividad que pudiera ser ilícita contactar con Fuerzas y Cuerpos de Seguridad del Estado. Informar de actividades ilícitas si la gravedad y categorización lo requiere a los entes de notificación externa como es el ColCERT - CSIRT
6. Reflexión y Mejora Continua

Documentación y almacenamiento a la base de datos del proceso de respuesta a incidentes apoyado con un resumen ejecutivo

Documentar los errores técnicos y procesos cometidos durante la gestión del incidente y las posibles acciones de mejora continua para la prevención y gestión de incidentes en el futuro.

Autor: Propio basado a la guía de la NIST SP.800-61r2 Computer Security Incident Handling Guide (NIST, 2020) y el centro criptológico nacional (Centro Criptológico Nacional, 2020)

ANEXO D¹⁸

ANEXO D¹⁹

14.15. Perfiles Sugeridos

14.15.1. Perfil Director

Perfil del Cargo	
Área:	Dirección de Seguridad y Ciberseguridad
Nombre cargo:	Director(a) de Seguridad y Ciberseguridad - CISO
Nivel de reporte:	Directo
Cargo superior:	Vicerrector
Rol organizacional:	Directivo
Propósito General	
Deberá garantizar la protección, calidad y veracidad de la información. Así mismo tendrá la responsabilidad de intervenir para salvaguardar los datos de posibles amenazas internas/externas	
Responsabilidades	

¹⁸ Autores y empresa ITFIP

¹⁹ Autores

Funciones: Gestionar posibles riesgos o incidentes que puedan afectar la seguridad y ciberseguridad de los sistema, implementar estrategias que garantizar la protección de la información, seguimiento y aseguramiento de normativas aplicadas a la organización y la ley, y realización de auditorías a diversas áreas de control.	
Alcance: Deberá ser capaz de tomar decisiones que afecten a la organización, supervisar los esquemas internos de seguridad y realizar intervenciones de ser necesario, divulgar política de buenas prácticas de seguridad en la organización, mitigar riesgos, gestionar incidentes de seguridad y establecer planes de contingencia periódicos.	
Parámetros para el éxito	
Mitigar la materialización de incidentes de Ciberseguridad generados por ciberataques o amenazas tecnológicas.	
Reducir debilidades y vulnerabilidades de las plataformas tecnológicas	
Reducir el apetito de riesgo de las plataformas tecnológicas.	
Reducir hallazgos de la contraloría y entes auditoria sobre lo procesos de Ciberseguridad.	
Reducir los riesgos de ciberseguridad y contenerlos adecuadamente.	
Derechos de decisión	
Propios	* Liderar la mesa de crisis para la gestión de incidentes de seguridad. * Gestionar los riesgos Cibernéticos y aplicar controles de seguridad

	* Definir la estrategia de Ciberseguridad para la entidad. * Dar conceptos y aprobaciones de implementaciones de TI bajo los parámetros de ciberseguridad y seguridad de la entidad. * Implementar controles que permitan mitigar los riesgos de Ciberseguridad de la entidad. * Aplicar políticas de Seguridad y Ciberseguridad a la entidad.
Propone o Influye	* Comunicaciones ante incidentes de Ciberseguridad/seguridad. * Propone e influye en la selección de proveedores de Ciberseguridad. * Propone e influye en el control de cambios. * Propone Políticas de seguridad que ayudan a mejorar el ambiente de control.
Otros Roles	
Participación y liderazgo de las mesas de crisis de gestión de incidentes.	
Participación en la identificación de Riesgos Cibernéticos y definición de planes de trabajo.	
Participar en la definición y ejecución de auditorías internas.	
Participación en nuevos proyectos y estrategias de la entidad, para garantizar correcta implementación de estándares.	
Guías de Acción	
Aplicar lo establecido en las políticas internas boletines, procesos y regulaciones existentes para el sector educativo y de gobierno. Permanecer actualizado en estas.	

Competencias	
Organizacionales	Específicas del Rol
- Resolución de conflictos: Identificar el problema y definir metodologías y toma de decisiones para la solución de este.	-Pensamiento crítico: Habilidad para generar múltiples análisis y posibles soluciones
- Liderazgo: Guiar a un equipo hacia el cumplimiento de metas, y promulgar el trabajo colectivo y la motivación.	- Atención: Rigurosidad para los detalles más mínimos y agilidad para ser capaz de atender los mismos.
- Trabajo en equipo: Cooperación entre diversos equipos de trabajo, y delegación de objetivos.	-Organización y Planeación: establecer objetivos, toma de decisiones, definición de tiempos y alcances de los procedimientos.

-Adaptabilidad: Modificación de decisiones y acciones para adecuarse a los retos de la organización.	-Comunicación: Debe ser capaz de expresar sus ideas a los colaboradores tanto de su área como externa.
Perfil Profesional	
Educación	
Ingeniería de Sistemas, informática, electrónica y/o afines con especialización en ciberseguridad o seguridad informática. Deseable: Maestría en Ciberseguridad o seguridad informática Deseable: Certificaciones en Ciberseguridad, ISO27001:2022, Cloud (AWS, Azure), Riesgos CRISK, CISSP, CISSM, CEH, GCIH.	
Experiencia	
3 años de experiencia en cargos Directivos y más de 5 años en áreas de Ciberseguridad TI y Seguridad informática. Experiencia en Ciberseguridad Experiencia en Gestión de incidentes de Ciberseguridad Experiencia en Seguridad Perimetral Experiencia en Sector Educativo /Entidades Públicas.	
Conocimientos específicos	

- * Asesorar a la organización para identificar, analizar y gestionar los riesgos asociados a ciberseguridad.
- * Diseñar e implementar estrategias de Ciberseguridad.
- * Diseñar soluciones de ciberseguridad mediante el uso de distintas herramientas del mercado.
- * Administración y seguimiento de proyectos.
- * Determinar las medidas de seguridad adecuadas para el tipo de información.
- * Explicar las medidas de seguridad implementadas a los empleados, utilizando un lenguaje no especializado.
- * Proteger información personal o confidencial del acceso o uso no autorizado
- * Reportar Gestionar y liderar incidentes de Ciberseguridad.
- * Desarrollar sistemas y protocolos de defensa como crear nuevas capas de protección, actualizar los sistemas de seguridad y desarrollar nuevos protocolos para contrarrestar las amenazas.
- * Ejecutar diagnósticos en los cambios de información en búsqueda de los trasposos o violaciones a los que haya habido lugar.
- * Elaborar informes de manera periódica sobre el estado de los sistemas.
- * Realizar pruebas en los sistemas y corregir toda debilidad o vulnerabilidad.

Referencias para el cargo

- Cano, J., & Almanza, A. (2023). Capacidades de los CISO's en Iberoamérica. Revista Sistemas. DOI: 10.29236/sistemas.n167a4
- Cuadra et, al. (2018). Tres Saberes en la Formación Profesional por Competencias: Integración de Teorías Subjetivas, Profesionales y Científicas. Citrevistas, Formación Universitaria, 11(5). Obtenido de <http://dx.doi.org/10.4067/s0718-50062018000500019>
- Gómez - Gamero , M. (2019). Las habilidades blandas competencias para el nuevo milenio. Divulgare Boletín Científico de la Escuela Superior de Actopan, 6(11). Obtenido de <https://repository.uaeh.edu.mx/revistas/index.php/divulgare/article/view/3760/5951>
- Hernández, C., & Nerí, J. (2020). Las habilidades blandas en estudiantes de ingeniería de tres instituciones públicas de educación superior. REDI, 48, supl. 1 . Obtenido de <http://doi.org/10.23913/ride.v10i20.678>
- Ramírez, M., & Manjarrez N. (2022). Habilidades blandas y habilidades duras, clave para la formación profesional integral. Universidad Técnica Estatal de Quevedo, Quevedo, Ecuador. Revista Ciencias Sociales y Económicas -UTEQ.

Autor: Propio

14.15.2. Perfil Profesional

Perfil del Cargo	
Area:	Dirección de Seguridad y Ciberseguridad
Nombre cargo:	Profesional Ciberseguridad
Nivel de reporte:	Directo
Cargo superior:	Director
Rol organizacional:	Profesional
Propósito General	
Deberá apoyar la protección, calidad y veracidad de la información. Así mismo tendrá la responsabilidad de intervenir para salvaguardar los datos de posibles amenazas internas/externas	
Responsabilidades	
Funciones: Apoyar en la gestión de posibles riesgos o incidentes que puedan afectar la seguridad y ciberseguridad de los sistema, implementar estrategias que garantizar la protección de la información, seguimiento y aseguramiento de normativas aplicadas a la organización y la ley, y realización de auditorías a diversas áreas de control. Alcance: Deberá tener capacidad de informar que afecten a la organización, validar los esquemas internos de seguridad y realizar intervenciones de ser necesario, divulgar política de buenas prácticas de seguridad en la organización, mitigar riesgos, gestionar incidentes de seguridad y establecer planes de contingencia periódicos.	

Parámetros para el éxito	
Mitigar la materialización de incidentes de Ciberseguridad generados por ciberataques o amenazas tecnológicas.	
Reducir debilidades y vulnerabilidades de las plataformas tecnológicas	
Reducir el apetito de riesgo de las plataformas tecnológicas.	
Reducir hallazgos de la contraloría y entes auditoria sobre lo procesos de Ciberseguridad.	
Reducir los riesgos de ciberseguridad y contenerlos adecuadamente.	
Derechos de decisión	
Propios	* Apoyar la gestión los riesgos Cibernéticos y aplicar controles de seguridad * Apoyar la estrategia de Ciberseguridad para la entidad. * Brindar conceptos y aprobaciones de implementaciones de TI bajo los parámetros de ciberseguridad y seguridad de la entidad. * Implementar controles que permitan mitigar los riesgos de Ciberseguridad de la entidad. * Aplicar políticas de Seguridad y Ciberseguridad a la entidad.
Propone o Influye	* Apoya la proposición e influye en la selección de proveedores de Ciberseguridad. * Apoya la proposición e influye en el control de cambios. * Apoya la proposición de Políticas de seguridad que ayudan a mejorar el ambiente de control.

Otros Roles	
Participación en la identificación de Riesgos Cibernéticos y definición de planes de trabajo.	
Participar en la definición y ejecución de auditorías internas.	
Participación en nuevos proyectos y estrategias de la entidad, para garantizar correcta implementación de estándares.	
Guías de Acción	
Aplicar lo establecido en las políticas internas boletines, procesos y regulaciones existentes para el sector educativo y de gobierno. Permanecer actualizado en estas.	
Competencias	
<i>Organizacionales</i>	<i>Específicas del Rol</i>
- Resolución de conflictos: Identificar el problema y definir metodologías y toma de decisiones para la solución de este.	-Pensamiento crítico: Habilidad para generar múltiples análisis y posibles soluciones
- Liderazgo: Guiar a un equipo hacia el cumplimiento de metas, y promulgar el	- Atención: Rigurosidad para los detalles más mínimos y agilidad para ser capaz de atender los mismos.

trabajo colectivo y la motivación.	
- Trabajo en equipo: Cooperación entre diversos equipos de trabajo, y delegación de objetivos.	-Organización y Planeación: establecer objetivos, toma de decisiones, definición de tiempos y alcances de los procedimientos.
-Adaptabilidad: Modificación de decisiones y acciones para adecuarse a los retos de la organización.	-Comunicación: Debe ser capaz de expresar sus ideas a los colaboradores tanto de su área como externa.
Perfil Profesional	
Educación	
Ingeniería de Sistemas, informática, electrónica y/o afines. Deseable: Certificaciones en Ciberseguridad, ISO27001:2022, Riesgos CRISK.	
Experiencia	

2 años de experiencia en cargos de Profesional o analista y más de 1 años en áreas de Ciberseguridad TI y Seguridad informática. Conocimiento en Ciberseguridad Conocimiento en Gestión de incidentes de Ciberseguridad Conocimiento en Seguridad Perimetral Conocimiento en Sector Educativo /Entidades Públicas.
Conocimientos específicos
* Apoyar en el diseño e implementar estrategias de Ciberseguridad. * Apoyar en el diseño soluciones de ciberseguridad mediante el uso de distintas herramientas del mercado. * Administración y seguimiento de proyectos. * Determinar las medidas de seguridad adecuadas para el tipo de información. * Explicar las medidas de seguridad implementadas a los empleados, utilizando un lenguaje no especializado. * Proteger información personal o confidencial del acceso o uso no autorizado * Reportar Gestionar los incidentes de Ciberseguridad. * Ejecutar diagnósticos en los cambios de información en búsqueda de los traspasos o violaciones a los que haya habido lugar. * Elaborar informes de manera periódica sobre el estado de los sistemas. * Realizar pruebas en los sistemas y corregir toda debilidad o vulnerabilidad.
Referencias para el cargo

Cano, J., & Almanza, A. (2023). Capacidades de los CISO's en Iberoamérica. Revista Sistemas. DOI: 10.29236/sistemas.n167a4

Cuadra et, al. (2018). Tres Saberes en la Formación Profesional por Competencias: Integración de Teorías Subjetivas, Profesionales y Científicas. Citrevistas, Formación Universitaria, 11(5). Obtenido de <http://dx.doi.org/10.4067/s0718-50062018000500019>

Gómez - Gamero , M. (2019). Las habilidades blandas competencias para el nuevo milenio. Divulgare Boletín Científico de la Escuela Superior de Actopan, 6(11). Obtenido de <https://repository.uaeh.edu.mx/revistas/index.php/divulgare/article/view/3760/5951>

Hernández, C., & Nerí, J. (2020). Las habilidades blandas en estudiantes de ingeniería de tres instituciones públicas de educación superior. REDI, 48, supl. 1 . Obtenido de <http://doi.org/10.23913/ride.v10i20.678>

Ramírez, M., & Manjarrez N. (2022). Habilidades blandas y habilidades duras, clave para la formación profesional integral. Universidad Técnica Estatal de Quevedo, Quevedo, Ecuador. Revista Ciencias Sociales y Económicas -UTEQ.

Autor: Propio

14.15.3. Perfil Analista

Perfil del Cargo	
Area:	Dirección de Seguridad y Ciberseguridad
Nombre cargo:	Analista Ciberseguridad
Nivel de reporte:	Directo
Cargo superior:	Profesional

Rol organizacional:	Analista
Propósito General	
Apoyar la protección, calidad y veracidad de la información. Así mismo tendrá la responsabilidad de intervenir para salvaguardar los datos de posibles amenazas internas/externas	
Responsabilidades	
Funciones: Apoyar en la gestión de posibles riesgos o incidentes que puedan afectar la seguridad y ciberseguridad de los sistema, implementar estrategias que garantizar la protección de la información, seguimiento y aseguramiento de normativas aplicadas a la organización y la ley, y realización de auditorías a diversas áreas de control. Alcance: Deberá tener capacidad de informar que afecten a la organización, validar los esquemas internos de seguridad y realizar intervenciones de ser necesario, divulgar política de buenas prácticas de seguridad en la organización, mitigar riesgos, gestionar incidentes de seguridad y establecer planes de contingencia periódicos.	
Parámetros para el éxito	
Reducir debilidades y vulnerabilidades de las plataformas tecnológicas	
Reducir el apetito de riesgo de las plataformas tecnológicas.	
Reducir los riesgos de ciberseguridad y contenerlos adecuadamente.	
Derechos de decisión	

Propios	* Apoyar la gestión los riesgos Cibernéticos y aplicar controles de seguridad * Brindar conceptos y aprobaciones de implementaciones de TI bajo los parámetros de ciberseguridad y seguridad de la entidad. * Aplicar políticas de Seguridad y Ciberseguridad a la entidad.
Propone o Influye	* Apoya la proposición e influye en la selección de proveedores de Ciberseguridad. * Apoya la proposición e influye en el control de cambios. * Apoya la proposición de Políticas de seguridad que ayudan a mejorar el ambiente de control.
Otros Roles	
Participación en nuevos proyectos y estrategias de la entidad, para garantizar correcta implementación de estándares.	
Guías de Acción	
Aplicar lo establecido en las políticas internas boletines, procesos y regulaciones existentes para el sector educativo y de gobierno. Permanecer actualizado en estas.	
Competencias	
<i>Organizacionales</i>	<i>Específicas del Rol</i>
- Resolución de conflictos: Identificar el problema y definir	-Pensamiento crítico: Habilidad para generar múltiples análisis y posibles soluciones

metodologías y toma de decisiones para la solución de este.	
- Trabajo en equipo: Cooperación entre diversos equipos de trabajo, y delegación de objetivos.	-Organización y Planeación: establecer objetivos, toma de decisiones, definición de tiempos y alcances de los procedimientos.
-Adaptabilidad: Modificación de decisiones y acciones para adecuarse a los retos de la organización.	-Comunicación: Debe ser capaz de expresar sus ideas a los colaboradores tanto de su área como externa.
Perfil Profesional	
Educación	
Tecnología de Sistemas, informática, electrónica y/o afines. Deseable: Certificaciones en Ciberseguridad, ISO27001:2022.	
Experiencia	

1 años de experiencia en cargos de analista y más de 1 años en áreas de Ciberseguridad TI y Seguridad informática. Conocimiento en Ciberseguridad Conocimiento en Gestión de incidentes de Ciberseguridad
Conocimientos específicos
* Apoyar en el diseño soluciones de ciberseguridad mediante el uso de distintas herramientas del mercado. * Aplicar las medidas de seguridad adecuadas para el tipo de información. * Explicar las medidas de seguridad implementadas a los empleados, utilizando un lenguaje no especializado. * Proteger información personal o confidencial del acceso o uso no autorizado * Reportar Gestionar los incidentes de Ciberseguridad. * Elaborar informes de manera periódica sobre el estado de los sistemas.
Referencias para el cargo

- Cano, J., & Almanza, A. (2023). Capacidades de los CISO's en Iberoamérica. Revista Sistemas. DOI: 10.29236/sistemas.n167a4
- Cuadra et, al. (2018). Tres Saberes en la Formación Profesional por Competencias: Integración de Teorías Subjetivas, Profesionales y Científicas. Citrevistas, Formación Universitaria, 11(5). Obtenido de <http://dx.doi.org/10.4067/s0718-50062018000500019>
- Gómez - Gamero , M. (2019). Las habilidades blandas competencias para el nuevo milenio. Divulgare Boletín Científico de la Escuela Superior de Actopan, 6(11). Obtenido de <https://repository.uaeh.edu.mx/revistas/index.php/divulgare/article/view/3760/5951>
- Hernández, C., & Nerí, J. (2020). Las habilidades blandas en estudiantes de ingeniería de tres instituciones públicas de educación superior. REDI, 48, supl. 1 . Obtenido de <http://doi.org/10.23913/ride.v10i20.678>
- Ramírez, M., & Manjarrez N. (2022). Habilidades blandas y habilidades duras, clave para la formación profesional integral. Universidad Técnica Estatal de Quevedo, Quevedo, Ecuador. Revista Ciencias Sociales y Económicas -UTEQ.

Autor: Propio

14.16. Presupuesto

Perfil o Rol	Salario Mensual	Costo Anual por Rol (COP)	Observación
Director	\$ 12.000.000	\$144.000.000	Aproximado
Profesional	\$ 8.000.000	\$96.000.000	Aproximado
Analista	\$ 5.000.000	\$ 60.000.000	Aproximado

Esto se saca de acuerdo con información pública de la página oficial de la “Función Pública”, DECRETO 2489 DE 2006, “Por el cual se establece el sistema de nomenclatura y clasificación de los empleos públicos de las instituciones pertenecientes a la Rama Ejecutiva y demás organismos y entidades públicas del Orden Nacional y se dictan otras disposiciones”²⁰

²⁰ Recuperado de <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=65341>

ANEXO E²¹**14.17. Gestión de Incidentes de Ciberseguridad**

Para el diseño del documento “Metodología de Gestión de Incidentes de Ciberseguridad para ITFIP”, se tuvo en cuenta las definiciones y estructura entregada en la Guía de Gestión de incidentes del MinTIC versión 2021, la cual a su vez tiene en cuenta la NIST 800-61, donde se permite definir los factores claves que se deben aplicar a la metodología de gestión de incidentes.

Con base en la guía (MinTIC, 2021), se logró hacer la estructuración del documento, donde se tuvo en cuenta lo siguiente:

- Objetivo
- Alcance
- Clasificación de incidente de Ciberseguridad
- CSIRT
- Roles y Responsabilidades
- Etapas del Incidente
- Comunicación

Permitiendo tomar como referencia este marco ya que es el que mejor se acomoda al ITFIP por el tipo de entidad ya que esta es publica y del sector gobierno vigilada por

²¹ Autores

el ministerio de Educación el cual está bajo los lineamientos del MINTIC en temas de Seguridad y Tecnología.

Adicionalmente por parte del CCN-STIC 817 - Esquema Nacional de Seguridad (Centro Criptológico Nacional, 2020) se tomó como referencia las definiciones de:

- Clasificación de incidente de Ciberseguridad
 - Tipo de amenaza
 - Origen de la amenaza
 - Categoría
 - Taxonomía y clasificación de incidentes de ciberseguridad.

Permite ayudar con el alcance de las terminologías y se adapta a lo que busca el ITFIP para su guía y manual de proceso de gestión de incidentes de ciberseguridad.

Finalmente, el marco general que abarca todo el proceso y la guía de gestión de incidentes de ciberseguridad del ITFIP está bajo la normativa de la NIST SP 800-61 (NIST, 2020) para revisar la documentación que está definida revisar los anexos X y X.

14.17.1. Introducción

El proceso de gestión de incidentes de Ciberseguridad cuenta con un enfoque documentado para que el ITFIP pueda dar una respuesta coordinada, ante un incidente de ciberseguridad y seguridad que pueda llegar a identificarse por causa de algún agente amenazante en las plataformas tecnológicas o que pueda comprometer a alterar la triada de

seguridad de la información (Confidencialidad, Integridad y Disponibilidad). Además, que permite definir una matriz de escalamiento para definir responsables desde la notificación/identificación hasta su cierre y documentación permitiendo aplicar las buenas prácticas con base en los marcos de referencia adoptados.

En los modelos de Ciberseguridad el proceso de gestión de incidentes es uno de los procesos más relevantes y críticos permitiendo definir un tema de aseguramiento en todas las etapas definidas en modelo de la NIST y por medio de las mejores prácticas, como lo es la guía de gestión de incidentes de Seguridad del MINTIC, el cual tiene un foco para entidades públicas que permite adaptarse a los temas exigidos por los estos reguladores. Se logra definir mecanismos y protocolos para la gestión de incidentes de ciberseguridad y seguridad, permitiendo establecer las diferentes etapas y actividades en el proceso.

14.17.2. Descripción

El proceso de gestión de incidentes de ciberseguridad y seguridad permite al ITFIP, tener definido el paso a paso de cómo actuar ante algún evento que se pueda materializar en un incidente de Ciberseguridad/seguridad, aplicando metodologías y buenas prácticas al proceso, permitiendo tener trazabilidad de todo el flujo desde la identificación hasta cierre y documentación, en donde se integran varias áreas de la entidad como se define en los roles y perfiles, aportando a minimizar el riesgo y controlarlo fortaleciendo los diferentes controles de seguridad que ayudan a bajar las probabilidades e impactos de la materialización de un incidente de ciberseguridad/seguridad.

14.17.3. Objetivo

El objetivo del proceso de gestión de incidentes es definir un modelo que permita al equipo de Tecnología del ITFIP tener la capacidad de coordinar y atender adecuadamente un incidente de ciberseguridad sobre las plataformas tecnológicas actuales, definiendo un flujo de trabajo, categorización de incidentes, escalamiento, definir tiempos de respuesta y dar priorización a los eventos reportados para mitigar los impactos que afecten la infraestructura tecnológica de la institución.

14.17.4. Alcance

El diseño propuesto de la gestión de incidentes de Ciberseguridad en referencia a los modelos o estándares anteriormente mencionados en el documento; se limita el alcance propuesto a los sistemas de información críticos de la infraestructura de la ITFIP, con ello abarcando sistemas Core de infraestructura, portales web donde reposa información valiosa de la organización, así como los servicios de academia (Core de negocio).

14.17.5. Referencia

El desarrollo de esta propuesta del presente documento tiene como soporte las metodologías y estándares nacionales e internacionales propuestas en el marco de referencia y de la misma forma la referencia de los organismos de control, las entidades de gobierno y leyes referenciadas en el marco legal.

14.17.6. Guías

En la elaboración y definición del siguiente procedimiento se toma como referencia las siguientes guías en lista.

- Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información, con relación a la seguridad y privacidad de la información, gobierno digital de la MinTIC. (MinTIC, 2021)
- Computer Security Incident Handling Guide NIST SP 800-61 R2. (NIST, 2020)
- Information technology —Information security incident management — Part 1: Principles and process. (ANSI, 2023)
- Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response. (ANSI, 2023)

14.17.7. Términos y Definiciones

- **Evento:** Ocurrencia o cambio de un conjunto particular de circunstancias, puede ser esperado o inesperado. (ISO/IEC, 2022)
- **Incidente:** Eventos únicos o una serie de eventos de seguridad no deseados o inesperados que tiene una probabilidad significativa de comprometer operaciones comerciales y amenazar la ciberseguridad/seguridad. (ISO/IEC, 2022)
- **CISO:** Chief Information Security Officer.
- **Riesgo:** Efecto de incertidumbre sobre un activo informático. (ISO/IEC, 2022)

- **Amenaza:** Causa potencial de un incidente de ciberseguridad/seguridad que puede provocar daños a un sistema o una organización (ISO/IEC, 2022)
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado y generar un evento u ocurrencia. (ISO/IEC, 2022)

14.17.8. Clasificación de Incidentes de Ciberseguridad/Seguridad

De acuerdo con las buenas prácticas y como lo menciona CCN-STIC-817, en su guía Esquema Nacional de Seguridad - Gestión de Ciber incidentes, se debe disponer de una taxonomía que permita clasificar los tipos de incidentes de seguridad permitiendo una mayor atención en el proceso de identificación. (Centro Criptológico Nacional, 2020).

14.17.9. Tipo de Amenaza

Es importante que se identifiquen los tipos de amenaza a los que está expuesta la entidad para tener un actuar más efectivo sobre el incidente, algunos de los que se tienen identificados son:

- Código malicioso
- Ransomware
- Intrusiones
- DDOS -DOS
- Otros.

14.17.10. Origen de la amenaza

Es importante determinar si el vector de ataque es un factor interno y externo para tomar medidas determinadas y contener el incidente mientras se ejecutan los controles de seguridad correspondientes y se hace el escalamiento a los responsables.

14.17.11. Categoría

Tener identificado y clasificados los activos de información de que permita identificar si es o no un activo crítico (Core de negocio) y puede generar impacto en la operación de la institución.

14.17.12. Perfil de usuario

Una vez se identifica que usuarios son objetivos del ataque que genera el incidente, se debe validar en que parte del esquema organizacional está ubicado y se debe entrar a validar sus accesos, validar los privilegios con los que cuenta a los sistemas de información, si maneja o no información confidencial de la institución.

14.17.13. Requerimientos legales.

Se debe validar si los activos e información afectada por el incidente aplica a alguna regulación sobre el reporte de incidentes y si estos fueron afectados o no de acuerdo con la criticidad de los activos y su información.

14.17.14. Taxonomía de clasificación los incidentes de ciberseguridad/seguridad.

Con base en la taxonomía propuesto por CCN-STIC-817, en su guía Esquema Nacional de Seguridad - Gestión de Ciber incidentes, se toma como referencia para definirlo a los casos prácticos que le aplican al ITFIP, como se muestra en la siguiente tabla:

Clasificación	Tipos de Incidente	Descripción
Contenido abusivo	SPAM	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
	Delito Informático	Contenido difamatorio o discriminatorio. Ejemplo: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
	Contenido no apropiado (sexual o violento inadecuado)	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
Contenido dañino	Sistema infectado	Sistema infectado con malware. Ejemplo: Sistema, computadora o teléfono móvil infectado con un rootkit.

	Servidor C&C (Mando y Control)	Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Distribución de malware	Recurso usado para distribución de malware. Ejemplo: recurso de una organización empleado para distribuir malware.
	Configuración de malware	Recurso que aloje ficheros de configuración de malware Ejemplo: ataque de webinjects para troyano.
	Escaneo de redes (scanning)	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ejemplo: peticiones DNS, ICMP, SMTP, escaneo de puertos.
Obtención de información	Análisis de paquetes (sniffing)	Observación y grabación del tráfico de redes.
	Ingeniería social	Recopilación de información personal sin el uso de la tecnología. Ejemplo: mentiras, trucos, sobornos, amenazas.

	Explotación de vulnerabilidades conocidas	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ejemplo: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).
Intrusión	Intento de acceso con vulneración de credenciales	Múltiples intentos de vulnerar credenciales. Ejemplo: intentos de ruptura de contraseñas, ataque por fuerza bruta.
	Ataque desconocido	Ataque empleando exploit desconocido.
	Compromiso de cuenta con privilegios	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Compromiso de cuenta sin privilegios	Compromiso de un sistema empleando cuentas sin privilegios.
	Compromiso de aplicaciones	Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ejemplo: inyección SQL.
	Robo	Intrusión física.

		Ejemplo: Robo a Centro de Proceso de Datos.
Disponibilidad	DDoS (Denegación distribuida de servicio)	Ataque de denegación distribuida de servicio. Ejemplo: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
	DDoS (Denegación distribuida de servicio)	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ejemplo: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto
	Mala configuración	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ejemplo: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto
	Sabotaje	Sabotaje físico.

		Ejemplo: cortes de cableados de equipos o incendios provocados.
	Interrupciones	Interrupciones por causas ajenas. Ejemplo: desastre natural.
Compromiso de la información	Acceso no autorizado a información	Acceso no autorizado a información. Ejemplo: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
	Modificación no autorizada de	Modificación no autorizada de información. Ejemplo: modificación por un atacante empleando credenciales sustraídas de un sistema o
	información	aplicación o encriptado de datos mediante Ransomware.
	Pérdida de datos	Pérdida de información Ejemplo: pérdida por fallo de disco duro o robo físico.
	Uso no autorizado de recursos	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej: uso de correo electrónico para participar en estafas piramidales.

	Derechos de autor	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor.
	Suplantación	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
Fraude	Phishing	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
		Servicios accesibles públicamente que puedan presentar criptografía débil. Ejemplo: servidores web susceptibles de ataques
	Criptografía débil	POODLE/FREAK.
Vulnerable	Amplificador DDoS	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ejemplo: DNS open- resolver o Servidores NTP con monitorización monlist.
	Servicios con acceso potencial no deseado	Ejemplo: Telnet, RDP o VNC.

	Revelación de información	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ejemplo: SNMP o Redis.
	Sistema vulnerable	Sistema vulnerable. Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
Otros	Otros	Todo aquel incidente que no tenga cabida en ninguna categoría anterior.
	APT	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

Autor: Tomado de la Guía de Seguridad de las

- Esquema Nacional de Seguridad. Gestión de ciber incidentes para aplicar a los casos que pueden presentarse en el ITFIP. (Centro Criptológico Nacional, 2020)

14.17.15. CSIRT

Para el ITFIP el CSIRT (Computer Security Incident Response Team) en español conocido como equipo de respuesta a incidentes, es el que opera para tratar y responder ante los incidentes de ciberseguridad/seguridad con el personal y recursos disponibles. Este equipo este compuesto por varias personas de diferentes áreas que aportan al proceso de acuerdo con las capacidades y habilidades dentro de la institución, según como se definió en su conformación.

14.17.16. Estructura del CSIRT

El equipo de respuesta a incidentes del ITFIP debe estar conformado principalmente por el CISO/Líder CSIRT y acompañado por el personal designado de las siguientes áreas:

- Tecnología.
- Comunicaciones.
- Legal.
- Alta Dirección.

14.17.17. Líder CSIRT

El líder del CSIRT por lo general es responsable de toma de decisiones claves para el proceso de atención al incidente de ciberseguridad/seguridad y también está en la capacidad de activar el equipo de gestión de incidentes si es el caso y permite tener comunicación directa con la alta dirección.

14.17.18. Roles y Responsabilidades

Los roles y responsabilidades definidos y propuestos para la universidad permiten que se tenga orientación y apoyo en los temas gestión del incidente de ciberseguridad/seguridad, apoyan en la actualización y mejora continua del proceso y las actividades para cada caso, identificar fallas, reportar y garantizar el cumplimiento de lo definido a nivel procedimental.

También permiten que se tenga un apoyo de equipos y áreas con conocimientos técnicos de acuerdo con el tipo de incidente que se llegue a presentar.

Todos los participantes del CSIRT deberán aportar uno de los factores según el rol desempeñado:

- Análisis de la situación.
- Identificación y de causa raíz del incidente
- Participar en las mesas de gestión de incidentes para toma de decisiones.
- Recopilación de logs y entregar evidencias forenses
- Certificar la operación de las plataformas tecnológicas
- Certificar cierre del incidente y documentación correspondiente.

14.17.19. CISO – Responsable de Ciberseguridad/Seguridad -Responsable Grupo

Atención a Incidentes.

Responde a las consultas sobre los incidentes de seguridad del ITFIP que impacten de forma inmediata, y es el encargado de revisar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de

ciberseguridad/seguridad para poder ser presentados a los directivos. El Líder Grupo de Atención de Incidentes estará en la capacidad de convocar la participación de otros funcionarios de la organización cuando el incidente lo amerita (Prensa y Comunicaciones, Gestión de Talento Humano, Gestión Jurídica, Tecnología, Representante de las Directivas para el SGSI). (MINTIC, 2016)

También debe estar al tanto del cumplimiento de los demás perfiles mencionados y de revisar el cumplimiento de los procedimientos y mejores prácticas, así como también de los indicadores de gestión, y en capacidad de disparar si lo amerita planes de contingencia y/o continuidad. (MINTIC, 2016)

Finalmente, el Líder del Grupo de Atención de Incidentes será el responsable del modelo de Gestión de incidentes y debe estar en la capacidad de revisar todos los incidentes de seguridad y los aspectos contractuales que manejan el outsourcing del servicio. (MINTIC, 2016)

14.17.20. Director de TI

El director de TI es el responsable de toda el área de Tecnología de la Universidad y debe estar presente para definir y tomar decisiones desde el ámbito tecnológico y entregar y organizar los equipos que hagan parte del proceso desde su frente para apoyar al Líder del Grupo de Atención de Incidentes.

Es responsabilidad del director de Tecnología que las aplicaciones, plataformas y servicios tecnológicos del ITFIP estén actualizados, y se cumpla lo definido por los lineamientos internos de C Ciberseguridad / Seguridad. Debe atender auditorias y velar por el buen funcionamiento de la tecnología y de cada herramienta designada.

14.17.21. Líder de Mesa de Ayuda

Es el responsable de recibir la notificación de primera mano de un posible incidente de ciberseguridad y seguridad si este es reportado por la mesa de servicio por algún usuario o personal interno de la universidad y debe garantizar que el equipo a cargo haga el escalamiento correspondiente para tomar acciones por los responsables de las herramientas definidas por el ITFIP.

14.17.22. Administrador de la Plataforma / Aplicación

Se define como la persona encargada para configurar y mantener un activo informático. También debe ser notificado por el agente de primer punto de contacto sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad. Este debe documentar y notificar al agente de primer punto de contacto sobre el incidente la solución de este. Se recomienda que los administradores cuenten con capacitación en Seguridad de la Información (con un componente tecnológico fuerte no solo en su plataforma si no en Redes y

erradicación de vulnerabilidades) y debe conocer perfectamente la clasificación de Incidentes y los procesos de escalamiento de Incidentes. Adicionalmente debe contar con una capacitación en técnicas forenses, específicamente en recolección y manejo de evidencia. (MINTIC, 2016)

14.17.23. Usuario Final

Es un empleado, empleados de firmas contratista o terceros con acceso a la infraestructura de la entidad, quien debe estar educado y concientizado sobre las guías implementadas sobre la seguridad de la información y en particular la guía de atención de incidentes, estos usuarios serán muchas veces quienes reporten los problemas (MINTIC, 2016).

14.17.24. Responsable Jurídico.

El responsable designado del área jurídica debe contar con conocimientos claros en las legislaciones, normas y temas regulatorios que competan a ciberseguridad, seguridad y privacidad para aportar en los comunicados a terceros, entes reguladores y asesorar al equipo para la correcta toma de decisiones.

14.17.25. Líder de Comunicaciones.

El responsable de comunicaciones debe apoyar a redactar y a notificar y hacer la divulgación de lo definido por el responsable Grupo Atención a Incidentes, una vez sea aprobado por la alta dirección / comité académico del ITFIP.

14.17.26. Etapas del Incidente

Con base en las guías de referencia nombradas en el punto 11.6 se da alcance a la adopción de etapas definidas a continuación:

14.17.27. Prevención y preparación

Frente a la prevención de acuerdo con la guía del MinTIC en su versión 2020 indica *“La entidad debe prepararse antes de la materialización de una amenaza, el equipo de Csirt Gobierno establece recomendaciones referentes a la configuración de últimas actualizaciones en sistemas operativos, servicios y aplicaciones. Es necesario que se cuenten con campañas de concienciación y sensibilización hacia los funcionarios en materia de ciberseguridad”* (MinTIC, 2021) lo cual se ajusta al ITFIP.

En la preparación de la gestión de incidentes no solo se debe tener en cuenta el tema de capacitación y concienciación como lo dice el MinTIC en su guía versión 2017 *“como pueden ser detectados, evaluados y gestionar las vulnerabilidades para prevenirse, asegurando que los sistemas, redes, y aplicaciones son lo suficientemente seguros .”* (MinTIC, 2021) por esta razón el equipo de respuesta a incidentes debe proceder bajo la experiencia de las buenas prácticas del aseguramiento de las plataformas y sistemas informáticos.

Entre las etapas de preparación que propone el MinTIC en su guía (MINTIC, 2016) y (MinTIC, 2021) están las siguientes:

- **Gestión de parches de seguridad:** Contar con un sistema de gestión de vulnerabilidades (Sistemas operativos, Bases de Datos, Aplicaciones, Código Fuente, Herramientas de apoyo, etc) (MINTIC, 2016) y (MinTIC, 2021) permitiendo tener una clasificación y tiempos de remediación.
- **Aseguramiento de plataforma:** En esto el MinTIC hace referencia a garantizar el mínimo privilegio sobre los usuarios creados en cada plataforma y sistema de información, verificar las configuraciones por defecto y aplicar las guías de hardening del fabricante o estandarizadas con los controles de seguridad correspondientes, basado en las buenas prácticas. (MINTIC, 2016) y (MinTIC, 2021).
- **Seguridad en Redes:** El MinTIC recomienda garantizar buena gestión sobre los equipos de seguridad perimetral como Firewall, IDS e IPS, donde se haga un constante afinamiento de reglas, y actualización de firmas para que los equipos operen y funcionen adecuadamente alertando de nuevas amenazas o IoC (Indicadores de compromiso), finalmente hacer todo el tema de recolección de logs a un centralizador de eventos para ser analizados y correlacionados. (MINTIC, 2016) y (MinTIC, 2021).

- **Prevención en código malicioso:** De acuerdo con lo menciona por el MinTIC se debe contar con un antivirus o antimalware con firmas actualizadas para identificar nuevas amenazas (MINTIC, 2016) y (MinTIC, 2021). Adicional a esto contar con herramientas más sofisticadas como lo son EDR (Endpoint Detection Responde) que permite hacer análisis basado en comportamientos e identificar cuando se está utilizando un vector de ataque sobre un Endpoint o servidor.
- **Sensibilización y entrenamiento de usuarios:** De acuerdo con lo mencionado por el MinTIC todo el personal de la entidad debe estar dentro de las capacitaciones de sensibilización sobre ciberseguridad, seguridad y gestión de incidentes de manera periódica, donde se explique las políticas internas de la entidad con alcance en redes, sistemas, aplicaciones, control de acceso y demás componentes de seguridad que son fundamentales para el manejo procesamiento y almacenamiento de información (MINTIC, 2016) y (MinTIC, 2021).

14.17.28. Detección

En este apartado la entidad, según el MinTIC en la guía recomienda tener los indicadores que señalen algunos de estos elementos claves para identificar un evento de seguridad (MinTIC, 2021):

- Alertas en sistemas de seguridad.
- Caídas o indisponibilidad de servidores.
- Reporte de usuarios por medio de mesa de servicio, llamada o correo electrónico.
- Alertas de agentes de antimalware, antivirus o EDR.
- Alertas de herramientas de seguridad definidas para cada propósito.

La gestión e identificación de las alertas presentadas sobre un incidente de ciberseguridad permiten proveer información que puede predecir ocurrencias futuras sobre este para minimizar su impacto y el Mintic nos recomienda los siguientes (MinTIC, 2021):

- Logs de servidores
- Logs de aplicaciones
- Logs de Bases de Datos
- Logs de herramientas de seguridad
- Logs que se centralicen en el SIEM de acuerdo con los casos de uso definidos.

14.17.29. Contención Erradicación y Recuperación

En esta fase se permite evitar la propagación del incidente y disminuir los daños que se puedan causar frente a la pérdida de integridad, disponibilidad y confidencialidad. (MinTIC, 2021)

- **Contención**

Permite identificar un incidente de seguridad con el fin de evitar su propagación y genere algún tipo de afectación, para esto el ITFIP cuenta con una estrategia de contención previamente definida donde se define una tomade decisiones entre estas esta:

- Apagado de sistemas.
- Aislamiento de la red
- Deshabilitar uno o los servicios asociados.
- Bloqueo de cuentas.
- Aplicar reglas de firewall específicas sobre un activo o IP.
- Agregar indicadores de compromiso asociados a IPs maliciosas.
- Generar casos de uso específicos en el SIEM.
- Generar alertamiento específico para toma de decisiones.

- **Erradicación y Recuperación**

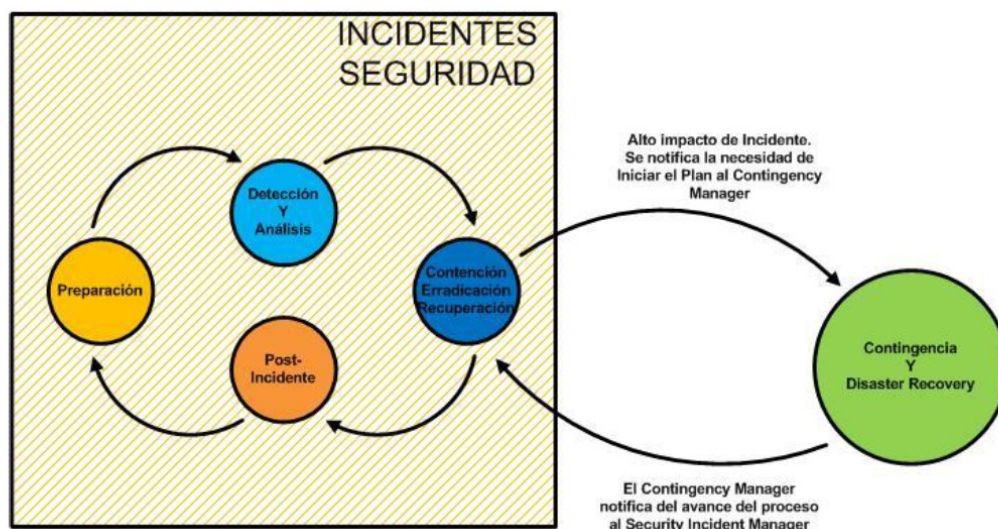
La erradicación se debe realizar de manera gradual para priorizar los pasos de remediación del incidente de ciberseguridad, se debe hacer una eliminación de cualquier rastro dejado por incidente como malware, o data afectada para proceder con la recuperación de manera correcta en un ambiente nuevo limpio y generar restauración de Backups si es el caso.

Algunas estrategias que se pueden optar para erradicar y recuperarse de un incidente de ciberseguridad pueden ser:

- Restitución de un servicio caído en caso de un DoS DDoS
- Corrección de efectos productivos y restauración de Backups en caso de ser afectados por un malware (virus gusano, troyano o Ransomware)
- Reparar o restaurar un sitio web por una excitación de Defacement al sitio Web de la institución.
- Reinstalación del equipo y recuperación de datos por una intrusión a algún sistema de información.

De acuerdo con lo recomendado por el MinTIC *“se puede hacer necesario activar el BCP (Plan de Continuidad del Negocio) o el DRP (Plan de Recuperación de Desastres) en el caso que un incidente afecte gravemente a un determinado sistema”*, por esto se alinea a los programas de BCP y DRP definidos por el ITFIP, para activar en caso de ser necesario.

A continuación, se ilustra el flujo de activación del BCP y DRP, como recomienda el MinTIC en la Guía de Gestión de Incidentes de la versión 2021:



Autor: (MinTIC, 2021)

14.17.30. Actividades Post incidente-Lecciones Aprendidas

En el proceso de gestión de incidentes es importante tener una mejora continua en todo el ciclo de vida del incidente identificado. Por esta razón se debe hacer un proceso de investigación que permita identificar la causa raíz del incidente y se documente de tal manera que pueda apoyar un futuro incidente y alimente la base de conocimiento de incidentes de seguridad definida por el ITFIP, finalmente muchas de estas investigaciones generan planes de acción o mejora, que permiten que la seguridad del ITFIP sea mayor y permita asegurar los sistemas de información.

Los incidentes de seguridad categorizados como críticos que generen afectación deben ser reportados al COLCERT de acuerdo con lo definido por el MinTIC.

- **Lecciones Aprendidas**

Contar con la fase de lecciones aprendidas en el proceso de gestión de incidentes permite mantener un adecuado registro y permite conocer los siguientes puntos recomendados por el MinTIC (MinTIC, 2021):

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Los procedimientos documentados.
- Si se tomaron las medidas o acciones que podrían haber impedido la recuperación.
- Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.
- Acciones correctivas pueden prevenir incidentes similares en el futuro.
- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro

Toda esta información se encuentra en el documento de apoyo “Anexo E” el cual se definió para tener soportado todo el proceso del incidente desde su identificación hasta su cierre y documentación.

14.17.31. Diagrama Etapas Definidas para la Gestión de Incidentes de Ciberseguridad.

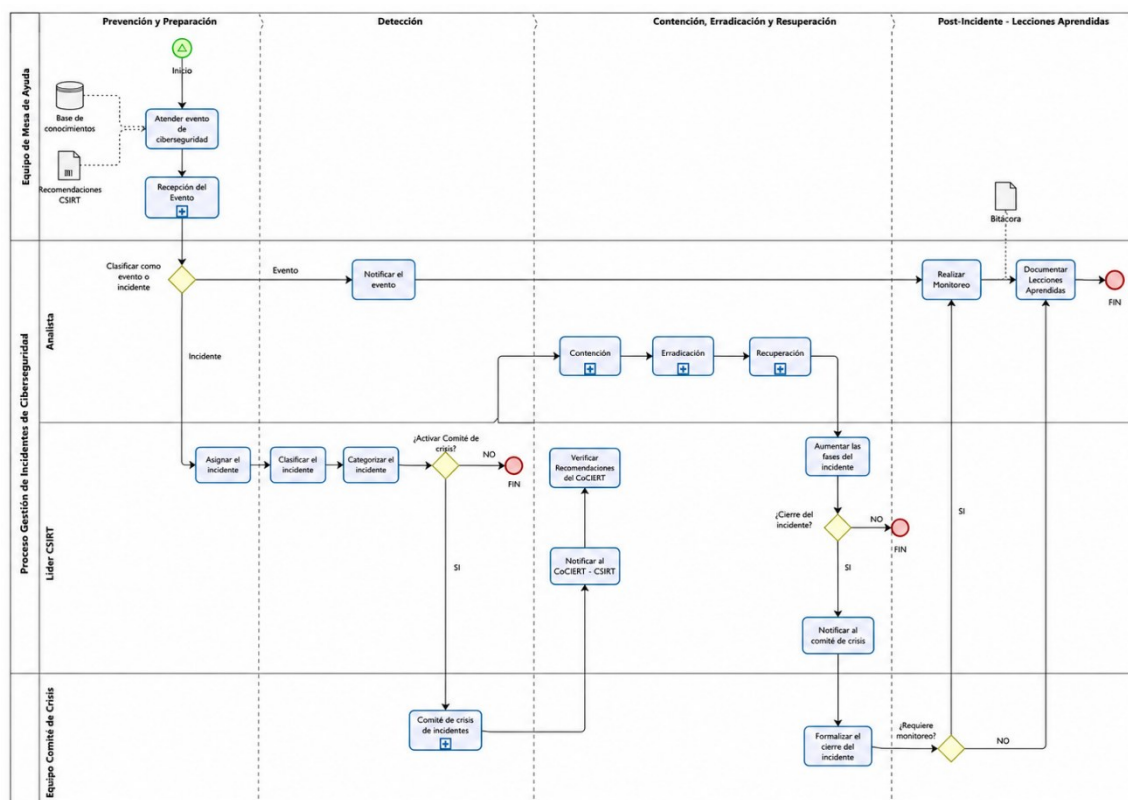


Ilustración 19 Proceso de Gestión de Incidentes de Ciberseguridad

Autor: Propio basado en la guía de MinTIC y NIST – Definición formal de la guía propuesta para la gestión de incidentes de ciberseguridad.

14.17.32. Medición

Las métricas definidas para la gestión de incidentes de Ciberseguridad permiten que se pueda medir el proceso y la gestión de cada una de las etapas identificadas en la gestión de incidentes de ciberseguridad al interior de la institución y permite genera planes de mejora que ayuden a la mejora continua. A continuación, se listan las métricas definidas:

- Tiempo de Respuesta del Incidente

Indicador	Tiempo de Respuesta del Incidente de Ciberseguridad.
Objetivo	Determinar el tiempo que toma el equipo en atender el incidente de ciberseguridad.
Medición	Promedio de la duración en minutos de cada incidente de ciberseguridad presentado desde el reporte hasta el cierre.
Caracterización	Se permite medir la eficiencia del equipo en la respuesta del incidente.
Frecuencia	Trimestral
Tipo	Métrica

Fuente: Autores

- Cantidad de incidentes de Ciberseguridad resueltos o cerrados

Indicador	Cantidad de incidentes de Ciberseguridad resueltos o cerrados
Objetivo	Medir la cantidad de incidentes resueltos.
Medición	Cantidad de Incidentes resueltos o cerrados / Cantidad de Incidentes Reportados
Caracterización	Permite medir la capacidad del equipo para resolver los incidentes de ciberseguridad.
Frecuencia	Mensual
Tipo	Métrica

Fuente: Autores

- Incidentes de Ciberseguridad Falsos positivos

Indicador	Incidentes de Ciberseguridad Falsos positivos
Objetivo	Medir la cantidad de falsos positivos reportados para la gestión de incidentes.
Medición	Cantidad de Incidentes categorizados como falsos positivos / Cantidad de Incidentes Reportados

Caracterización	Permite identificar si se está realizando un adecuado reporte de los incidentes de ciberseguridad.
Frecuencia	Trimestral
Tipo	Métrica

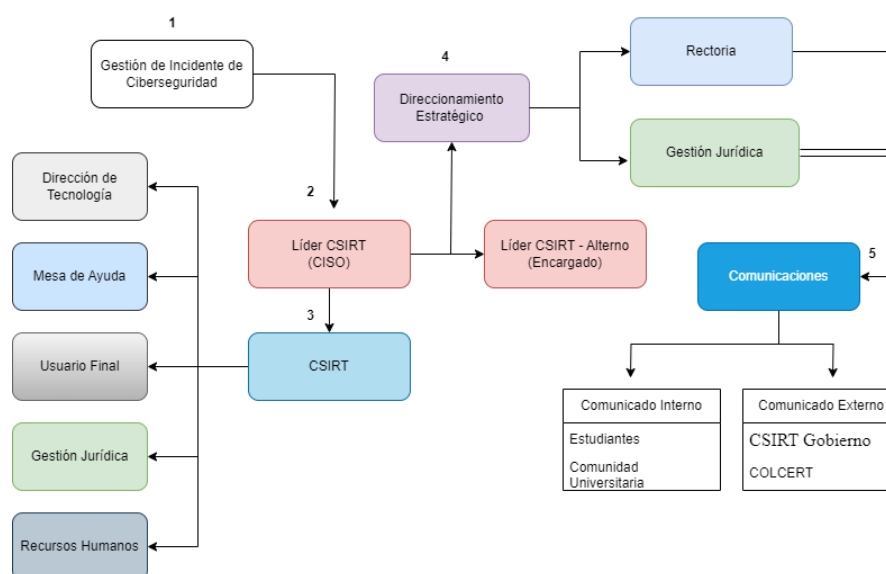
Fuente: Autores

14.17.33. Comunicación del Incidente

14.17.34. Interna

Para la comunicación interna en caso de presentar un incidente de ciberseguridad se definió el siguiente diagrama, como se evidencia en la imagen :

Flujo de Comunicación al CSIRT



Fuente: Autores

Tabla con actividades y acciones de cada una de las actividades de comunicación del incidente.

#	Activación	Acción / Definiciones
1	Gestión de Incidente de Ciberseguridad	Es el proceso donde se identifica el evento se clasifica y se categoriza para generar el reporte del incidente si este se materializa o se identifica según el análisis previo.
2	Líder CSIRT	Responsable de recibir la notificación de primera mano para determinar si se requiere activar el equipo de respuesta a incidentes.
3	CSIRT	Equipo multidisciplinario que hace parte del incidente desde su identificación y reporte, para dar detalle y definir el impacto.
4	Direccionamiento Estratégico	Es la alta Dirección del ITFIP asesorada del área Jurídica para determinar la comunicación del incidente y toma de decisiones de

		acuerdo con el Core de negocio del ITFIP
5	Comunicaciones	Área responsable de redactar los comunicados internos y externos con base en la información suministrada por el Líder CSIRT y Direccionamiento Estratégico.

Fuente: Autores

Adicionalmente, se debe tener en cuenta que para genera un reporte de un posible evento o incidente de ciberseguridad identificado al interior del ITFIP:

Origen de Reporte	Medio del Reporte	Detalle
Personal Administrativo	Correo Electrónico	Para: Mesa_ayuda@itfip.gov.co
Personal Docente		CC eventos_ciberseguridad@itfip.gov.co
Estudiantes / Egresados		

Contratistas / Proveedores	Teléfono	Extensiones de mesa de servicio definida por el ITFIP.
	Herramienta	
	TIC	URL: mesadeayuda.itfib.glpi.gov.co

Fuente: Autores

14.17.35. Externa

De acuerdo con lo estipulado en la Guía de gestión de incidentes del MinTIC (MinTIC, 2021) menciona lo siguiente: *“cuando se considere pertinente, al Grupo de Respuesta a Emergencias Cibernéticas de las entidades del estado (CSIRT Gobierno) o quien haga sus veces, además de reportar a su CSIRT sectorial, los incidentes de seguridad Digital que requieran de su gestión por medio de correo electrónico a: csirtgob@mintic.gov.co o al Teléfono: (+571) 2959897.”*

Cuando se tenga evidencia de un incidente cibernético, el ITFIP se debe poner en contacto con el CSIRT de gobierno csirtgob@mintic.gov.co, para recibir asesoría del caso en particular o directamente reportar al COLCERT (Grupo de Respuestas a Emergencias Cibernéticas de Colombia.)

Adicionalmente, se debe tener en cuenta que para genera un reporte de un posible evento o incidente de ciberseguridad identificado al exterior del ITFIP:

Origen de Reporte	Medio del Reporte	Detalle
Personal Externo o ajeno a la institución	Correo Electrónico Teléfono	Para: servicio_cliente@itfip.gov.co CC eventos_ciberseguridad@itfip.gov.co Al PBX del ITFIP opción Servicio al cliente, para retransmitir la información a las áreas correspondientes.
COLCER T (Grupo de Respuestas a	Correo Electrónico Teléfono	Comunicados: gobierno csirtgob@mintic.gov.co +57 601 344 34 60

Emergencias Cibernéticas de Colombia.)	Sitio de Reportes	https://www.colcert.gov.co/800/w3-article-198656.html#formulario_i_form_ReporteIncidentes_1 https://www.colcert.gov.co/800/w3-propertyvalue-466294.html
--	-------------------	--

Fuente: Autores

14.17.36. Control de Cambios

Historial de Cambios		
Versión	Fecha Publicación	Descripción del Cambio
1	30/06/2024	Se realiza creación del documento X.

Fuente: Autores

Matriz de Escalamiento:

Cargo	Nombre	Email	Rol	Sitio	Fijo	Celular	Temas
Analistas		-	Mesa de ayuda	Tolima			Escalamientos de ciberseguridad, primer punto de comunicación para escalamiento de todos los incidentes de seguridad
Proveedores		-	SOC, Mesa de ayuda	Tolima			Analítica Datos, Fortinet
Director de Tecnología		-	Proyecto TI	Tolima			Temas de servicio - Gestión de recursos - Quejas Cliente - Riesgos para el servicio

EN CUALQUIER HORARIO DE OFICINA

#	Nombre	Email Corporativo/Alternativo	Tipo Contacto	Disponibilidad	Ubicación	Teléfono Fijo	Teléfono Móvil
---	--------	----------------------------------	---------------	----------------	-----------	------------------	-------------------

1	Mesa de ayuda	mesadeayuda@itfip.edu.co	Por Correo Electrónico	5X8 (horario de oficina)	Tolima		
2		-	Operación e Incidentes de Ciberseguridad	5X8 (horario de oficina)	Tolima		
3		-	Director TI	5X8 (horario de oficina)			

En caso de indisponibilidad o Fallas en Servidores (Conectividad), en los Conectores caídos, que no lleguen eventos o algún servicio afectado en los servidores

#	Área de Seguridad	Nombre	Email Corporativo/Alternativo	Tipo Contacto	Disponibilidad	Teléfono Móvil
1	Ciberseguridad, Investigación Incidentes			Operación e Incidentes	5*8	
2	Ciberseguridad, Investigación Incidentes			Operación e Incidentes	5*8	
3	Ciberseguridad, Investigación Incidentes			Operación e Incidentes	5*8	

ANEXO F²²**14.18. Manual de Procedimiento****14.18.1. Flujo del incidente**

De acuerdo con la (ISO/IEC 27000, 2018) que define un Incidente como una serie de eventos de seguridad de la información únicos o una serie de eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información; de esta forma es una acción que causa la interrupción o reducción de un servicio que puede afectar como la disponibilidad, la integridad y la confidencialidad de la información, convirtiéndose en un incidente de seguridad.

En este tipo de escenario se propone un modelo del flujo de la gestión de eventos e incidentes que implica el plan de trabajo que reúne una serie de procedimientos enrolados a los partícipes de la operación desde el proceso en que inicia con la detección, identificación del evento en proceso, notificación de este, etapa de la recuperación, las actividades que se requieren después del incidente y por ultimo las lecciones aprendidas; así como lo referencia el estándar internacional de la ISO 27035. (ANSI, 2023)

La ITFIP tendrá la capacidad de poder reportar o notificar a la entidad del ColCERT -CSIRT aquellos incidentes de seguridad tanto internos como externos categorizados de

²² Autores

nivel alto y crítico de acuerdo con el tipo de clasificación y criticidad de los incidentes, ya sea de origen accidental o de forma malintencionada; esta notificación precisa la información que se debe suministrar, el tiempo o plazo requerido en la notificación y aquellos requisitos estándar para poder dar cumplimiento en términos legales de la notificación a la entidad; así como lo referencia y sugiere la guía para la gestión de y clasificación de incidentes de Seguridad de la Información, (MinTIC, 2021).

El modelo de la gestión de incidentes tiene como base hacer uso de las herramientas tecnológicas necesarias que dispone la organización para poder mitigar o contener cualquier tipo de amenaza y en el registro del evento de ciberseguridad.

Los usuarios, contratistas y terceros de la institución, de acuerdo con el uso de los sistemas de las tecnologías de la información, están en su deber de cuidar y velar por el cuidado de la salud de la infraestructura; y entre sus capacidades de poder notificar cada evento sospechoso del sistema al área o primer contacto definido por la organización. Estas notificaciones poder ser mediante cualquier canal de notificación formal que estipule la institución y con la mayor cantidad de información posible relacionada con el mismo. (MinTIC, 2021) en la declaración y notificación del Incidente.

En el modelo del flujo de la gestión de incidente en su primera etapa de la identificación y detección del incidente, consta de identificar el tipo de incidente de seguridad de la información, en este análisis se evalúa si corresponde a un nivel superior

de resolución, o está relacionado con requerimientos propios de la infraestructura, o falso positivo.

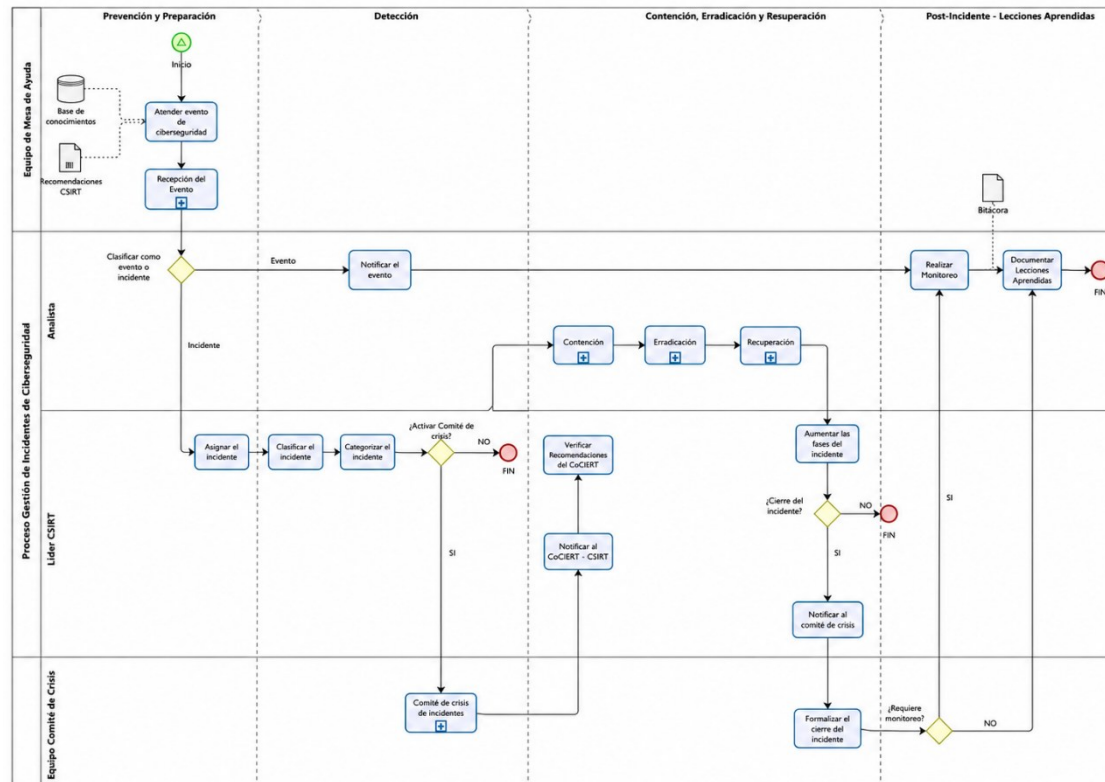
Luego de ser analizado el evento y ser categorizado como incidente de Seguridad, se notificará al directo responsable del equipo de respuesta a incidentes, para que tome las decisiones correspondientes, y será el encargado de realizar el seguimiento del Incidente hasta su cierre definitivo

Existe otra línea de detección del incidente diferente al usuario como son las plataformas de detección o el mismo personal de TI, donde notificara al personal encargado de la gestión de incidentes, quien realizara la documentación respectiva, las tareas de seguimiento y desarrollo de este. Así como se referencia en la atención de incidentes (MinTIC, 2021).

Es importante en la gestión de incidentes, el primer contacto que es la persona encargada de la notificación, esta misma la atención del mismo incidente; en sus tareas de coordinación a las partes interesadas, con el ello el equipo de respuesta a incidentes se apoyará con los dueños del proceso o personas involucradas para dar una correcta ejecución de actividades para la solución del incidente. Esta persona encargada con el rol de la gestión de incidentes tiene la potestad respecto a las decisiones que se tomen y en cada una de las acciones que se ejecutan en la presencia de un incidente de seguridad y este mismo rol será quién comunicara o notificará a la alta dirección de la institución; de acuerdo con lo mencionado en el equipo modelo o la estructura del equipo en la NIST. (NIST, 2023)

14.18.2. Flujograma Gestión eventos de Ciberseguridad y Seguridad

Ilustración 20 Proceso de Gestión de Incidentes de Ciberseguridad



Autor: Propio basado en la guía de MinTIC y NIST – Definición formal de la guía propuesta para la gestión de incidentes de ciberseguridad.

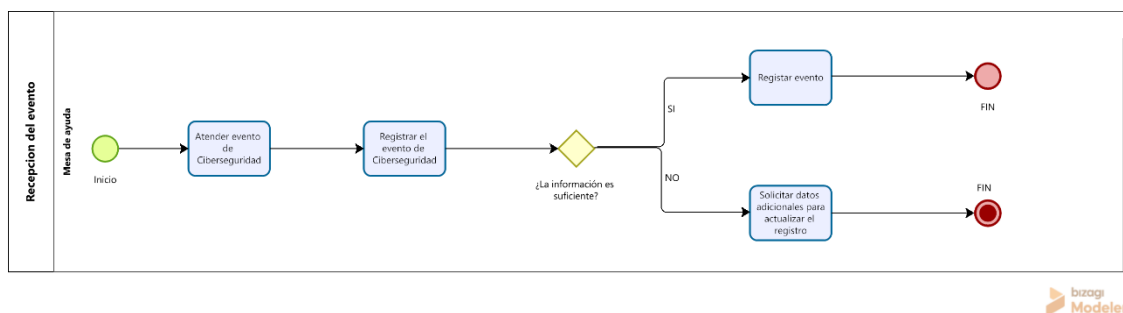
14.18.3. Subproceso – Recepción del Evento

Descripción: El diagrama presenta de manera estructurada y detallada el flujo del proceso, iniciando con la recepción del evento de ciberseguridad. Esta primera etapa contempla la atención del evento a partir de las diferentes fuentes de origen, como llamadas telefónicas, correos electrónicos o tickets generados en la plataforma GLPI.

Posteriormente, se lleva a cabo la actividad de registro del evento, la cual debe incluir la información mínima necesaria para su adecuada gestión, tales como un identificador único (ID), el usuario que reporta o notifica, la plataforma involucrada, entre otros datos relevantes.

En caso de que la información inicial sea insuficiente para la creación del ticket o caso, se deberá solicitar la información adicional requerida, garantizando así un registro completo y adecuado del evento de ciberseguridad.

Ilustración 21 Subproceso Recepción del evento



Autor: Propio basado en la guía de MinTIC y NIST – Definición formal de la guía propuesta para la gestión de incidentes.

14.18.4. Subproceso del Comité de Crisis del incidente de Ciberseguridad

Descripción: El diagrama representa el flujo de activación y operación del Comité de Crisis ante la ocurrencia de un incidente de ciberseguridad con impacto significativo para la institución ITFIP. Este proceso se integra dentro del modelo general de gestión de incidentes de Ciberseguridad, y tiene como propósito coordinar la toma de decisiones estratégicas, garantizar la continuidad del negocio y mitigar los efectos del incidente de manera oportuna.

El flujo inicia con la identificación de un incidente crítico, el cual, tras un proceso de evaluación inicial, cumple con los criterios para escalar a nivel de crisis. A partir de este punto, se activa formalmente el Comité de Crisis, involucrando a los diferentes actores clave de la institución.

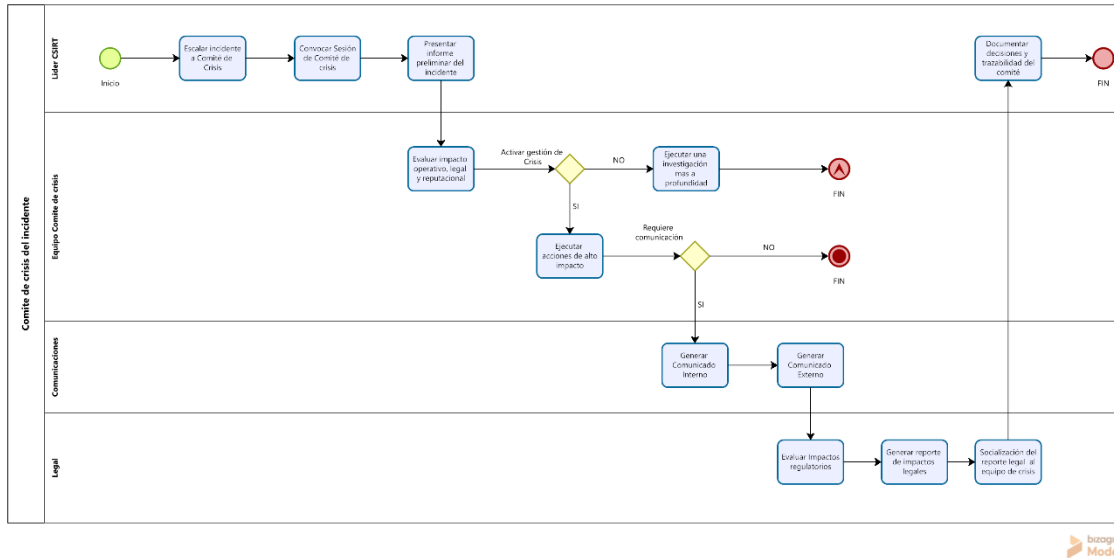
A lo largo del diagrama se describen las actividades principales del comité, que incluyen la convocatoria de los integrantes, la evaluación del impacto (operativo, reputacional, legal y tecnológico), la definición de estrategias de contención y comunicación, así como la asignación de responsabilidades para la ejecución de acciones inmediatas.

El modelo también establece claramente los roles participantes, tales como el equipo de comité de crisis, líderes de áreas técnicas, comunicaciones y legal. Cada uno de estos roles cumple funciones específicas dentro del proceso, permitiendo una gestión coordinada, eficiente y alineada con los objetivos organizacionales.

Asimismo, el flujo incorpora puntos de decisión clave, en los cuales se determina la evolución del incidente, la necesidad de escalamiento adicional, la interacción con terceros (como autoridades o proveedores) y la definición de planes de recuperación. Estas decisiones son fundamentales para adaptar la respuesta en función de la criticidad y evolución del incidente de ciberseguridad.

Finalmente, el proceso contempla el cierre del comité de crisis, una vez controlado el incidente, junto con la documentación de las acciones realizadas, decisiones, impactos legales y regulatorios, las cuales contribuyen al fortalecimiento continuo de las capacidades de respuesta ante futuros incidentes. Este diagrama constituye una guía estructurada para la gestión de crisis en ciberseguridad, facilitando la coordinación interáreas, la toma de decisiones informadas y la protección de los activos críticos de la organización.

Ilustración 22 Subproceso Comité de Crisis



Autor: Propio basado en la guía de MinTIC y NIST – Definición formal de la guía propuesta para la gestión de incidentes.

14.18.5. Subproceso de Contención

Descripción: El proceso de contención de incidentes de ciberseguridad, constituye una fase crítica dentro del ciclo de gestión de incidentes. Su objetivo principal es limitar la propagación del incidente, reducir su impacto en los activos de información y preservar la continuidad operativa de la institución ITFIP.

El flujo inicia una vez el incidente ha sido identificado y analizado preliminarmente, permitiendo activar las acciones de contención de manera oportuna. A partir de este punto, el proceso describe una serie de actividades técnicas y operativas

orientadas a aislar los sistemas comprometidos, restringir accesos no autorizados y evitar la escalabilidad de la amenaza.

A lo largo del diagrama se evidencian diferentes estrategias de contención, que pueden variar según la naturaleza del incidente, tales como la segmentación de redes, el bloqueo de cuentas o direcciones IP, la desactivación de servicios comprometidos y la aplicación de controles temporales de seguridad. Así mismo se cuenta con una base de datos de consulta de información que incluye guías y playbooks referente a la categorización del incidente como puede ser una intrusión, denegación de servicios, código malicioso, etc. estas acciones buscan estabilizar el entorno mientras se prepara la fase de erradicación.

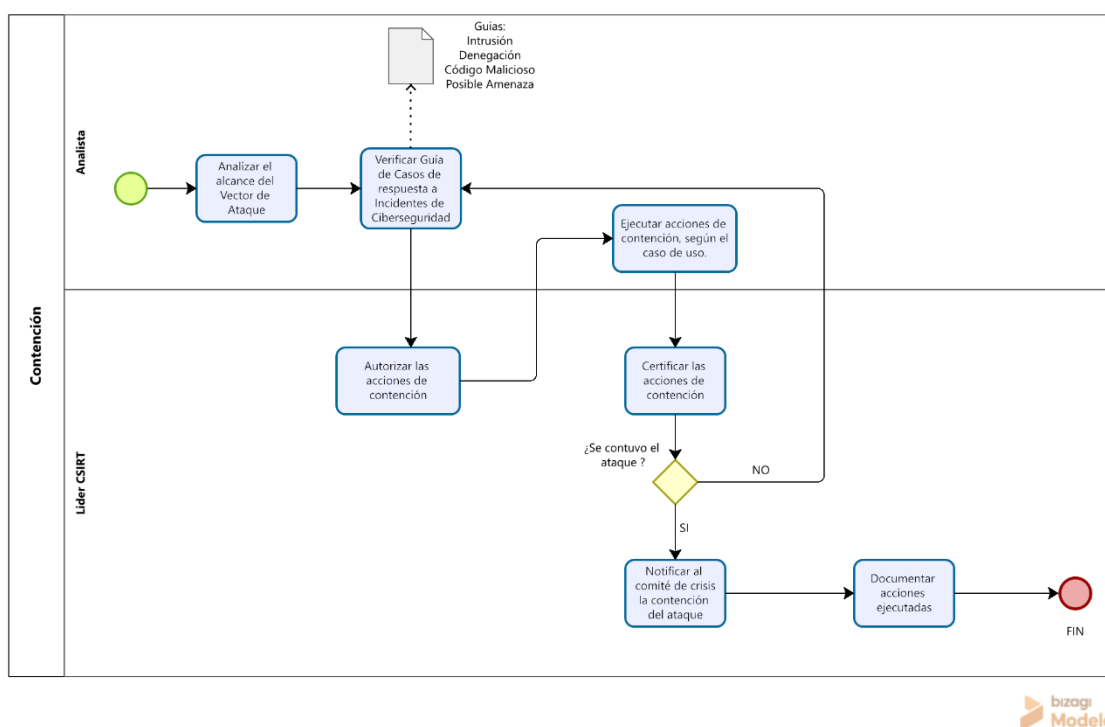
El modelo también define claramente los roles involucrados, líder CSIRT administradores de infraestructura, redes y sistemas, quienes actúan de forma coordinada para ejecutar las medidas de contención bajo lineamientos previamente establecidos.

Asimismo, el flujo incorpora puntos de decisión clave, donde se evalúa la efectividad de las acciones implementadas, la necesidad de escalar el incidente o de aplicar medidas adicionales. Estas decisiones permiten adaptar la respuesta en tiempo real, en función del comportamiento y alcance del incidente.

Finalmente, el proceso contempla la validación de la contención lograda, asegurando que la amenaza ha sido controlada de manera efectiva antes de dar paso a las siguientes fases del ciclo de gestión de incidentes, como la erradicación y recuperación.

Este diagrama proporciona una guía estructurada para la ejecución de acciones de contención, fortaleciendo la capacidad de respuesta de la organización frente a incidentes de ciberseguridad y minimizando los riesgos asociados a su propagación.

Ilustración 23 Subproceso Contención



Autor: Propio basado en la guía de MinTIC y NIST – Definición formal de la guía propuesta para la gestión de incidentes.

14.18.6. Subproceso Erradicación

Descripción: Este diagrama corresponde a una fase posterior a la contención y tiene como objetivo principal eliminar de manera definitiva la causa raíz del incidente, así como cualquier rastro de la amenaza dentro de la infraestructura tecnológica de la organización.

El flujo inicia una vez se ha logrado contener el incidente, permitiendo avanzar hacia la ejecución de acciones orientadas a la eliminación completa del agente malicioso, vulnerabilidades explotadas o accesos no autorizados que dieron origen al incidente de seguridad.

A lo largo del proceso se detallan diversas actividades técnicas especializadas, tales como la limpieza de sistemas comprometidos, eliminación de malware, aplicación de parches de seguridad y fortalecimiento de configuraciones en los activos impactados. Estas acciones buscan garantizar que el entorno quede libre de amenazas y que no existan mecanismos de persistencia que puedan generar una reincidencia del incidente.

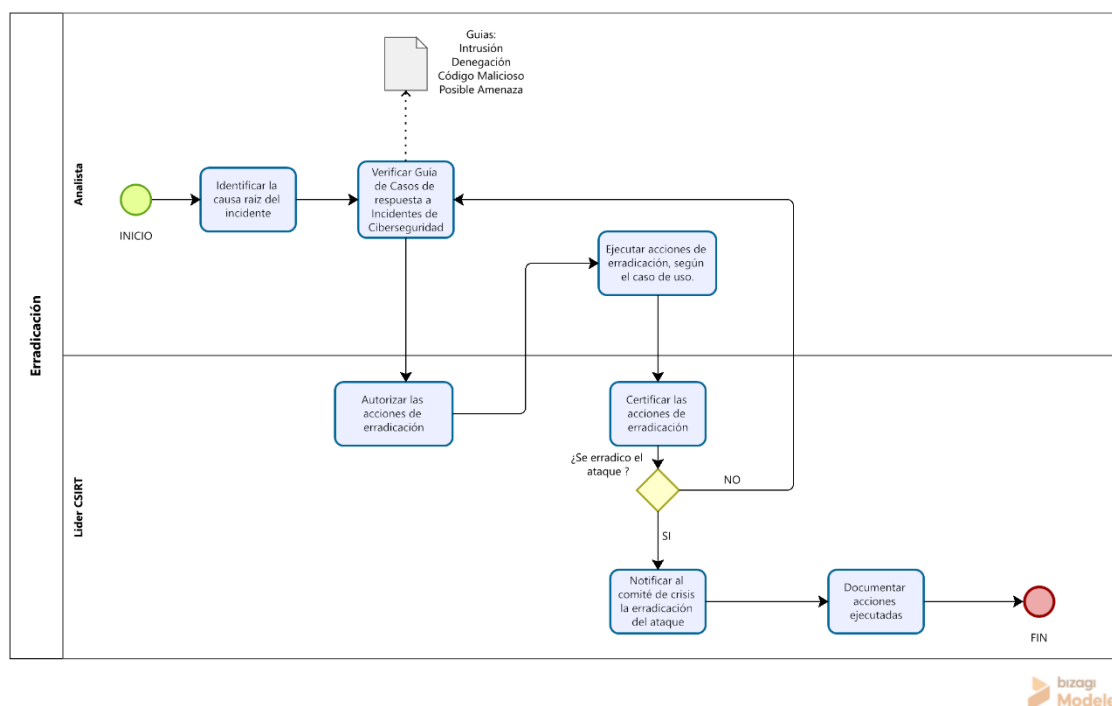
El modelo también establece los roles involucrados, líder CSIRT, administradores de infraestructura, quienes ejecutan las tareas de erradicación de forma coordinada y bajo procedimientos definidos.

Asimismo, el diagrama incorpora puntos de verificación y decisión, en los cuales se valida si la amenaza ha sido completamente eliminada o si es necesario repetir o reforzar

las acciones implementadas. Estas validaciones son fundamentales para asegurar la efectividad del proceso antes de avanzar a la fase de recuperación.

Finalmente, el proceso concluye con la confirmación de la erradicación del incidente, dejando el entorno en condiciones seguras y controladas para restablecer los servicios afectados. Esta fase es clave para prevenir la recurrencia del incidente y fortalecer las capacidades de respuesta de la organización frente a futuras amenazas.

Ilustración 24 Subproceso Erradicación



Autor: Propio basado en la guía de MinTIC y NIST – Definición formal de la guía propuesta para la gestión de incidentes.

14.18.7. Subproceso Recuperación

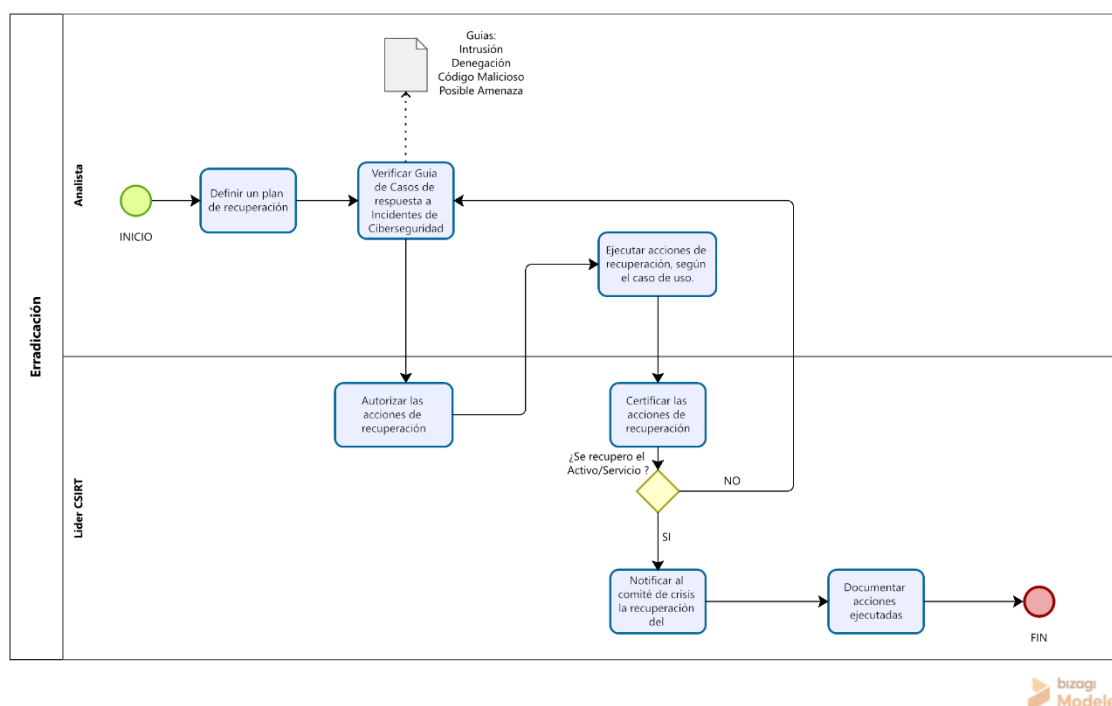
Descripción: La fase de recuperación dentro del proceso de gestión de incidentes de ciberseguridad, la cual tiene como propósito restablecer los servicios, sistemas y operaciones afectados, garantizando que estos vuelvan a un estado seguro, estable y controlado después de haber contenido y erradicado la amenaza.

El proceso inicia una vez se ha confirmado la eliminación del incidente, dando paso a la ejecución de actividades orientadas a la restauración de la operación normal. En esta etapa, los equipos técnicos proceden a la recuperación de los sistemas impactados, lo cual puede incluir la restauración de respaldos o backups, la reconfiguración de servicios, la validación de integridad de la información.

Las actividades en esta etapa pueden involucrar pruebas de funcionamiento, revisiones de seguridad, monitoreo intensivo y verificación de que los controles implementados continúan siendo efectivos. El diagrama también refleja la participación de distintos roles que conforman el comité de crisis como también , usuarios finales, quienes validan la correcta operación de los servicios restaurados. Esta interacción permite garantizar que la recuperación no solo sea técnica, sino también funcional desde el punto de vista del negocio.

Finalmente, el flujo concluye con la confirmación de la recuperación total del entorno afectado, asegurando que los servicios operan con normalidad y bajo condiciones seguras. Esta fase sienta las bases para el cierre formal del incidente y la posterior generación de lecciones aprendidas.

Ilustración 25 Subproceso Erradicación



Autor: Propio basado en la guía de MinTIC y NIST – Definición formal de la guía propuesta para la gestión de incidentes.

14.19. Niveles de atención de un incidente de ciberseguridad.

Se propone una estructura de equipo de atención de incidentes de ciberseguridad para el modelo definido y ajustado a la propuesta a la institución se toma como referencia (NIST, 2023).

En esta etapa se detalla nivel a nivel las responsabilidades quienes se involucran en la atención de un incidente, cada uno está en la potestad de poder registrar los incidentes presentados.

Nivel 0 - usuario:

Esta responsabilidad de lleva a cabo quien registra todos los incidentes de seguridad en la institución, a través de los canales de notificación (correo electrónico, llamada telefónica, ticket, etc.). En este punto debe escalar e informar oportunamente al primer contacto responsable de la gestión de incidentes de ciberseguridad.

Nivel 1 – Personal con conocimiento técnico de Ciberseguridad – Mesa de ayuda.

En este punto de atención de encarga de dar gestión sobre el reporte de un evento o incidente de seguridad de ciberseguridad desde cualquier ámbito, ejecutando acciones oportunas para contener, mitigar o erradicar las posibles fuentes de ataque, amenazas o vulnerabilidades explotadas que permitan la afectación de los sistemas en la afectación de la integridad,

confidencialidad y disponibilidad de la información sobre los activos de la institución. De esta forma también en el acompañamiento para el seguimiento o trazabilidad de la misma gestión del incidente y en la documentación de todas las acciones, cambios, registros respecto a los eventos e incidentes de ciberseguridad. Tomado como referencia (MinTIC, 2021). Declaración y notificación de incidentes.

Paso siguiente si no es responsable de la solución del incidente, procederá a escalarlo al dueño o directo responsable especializado del servicio, en otra medida la atención al equipo de respuesta o al comité de crisis de incidentes.

Nivel 2 – Equipo de respuesta de incidentes.

Equipo conformado por personas especializadas en la atención de incidentes, conformado por líderes de servicios, administradores responsables de la administración de sistemas de TI y seguridad, en este equipo son responsables de diagnosticar y resolver o participar en la resolución de los incidentes de seguridad de categorías con nivel Alto o crítico. (MinTIC, 2021) Declaración y notificación de incidentes.

Nivel 3- Gestión de Crisis

En esta etapa cubre una serie de responsabilidad y es basado en roles de cada una de las áreas respecto a incidentes de nivel crítico, cada persona líder o dueño del proceso está involucrado en este comité de crisis.

Tabla 20 Nivel de escalamiento

Nivel	Nombre	Contacto / Responsable
0	Usuario	Quien reporta el incidente / Usuario Final.
1	Personal con conocimiento técnico de Ciberseguridad – Mesa de ayuda.	Mesa de Ayuda equipo de TI asignado.
2	Equipo de respuesta de incidentes.	Áreas involucradas en el incidente de seguridad.
3	Gestión de Crisis	Líder CSIRT – (CISO)

Fuente: Autores

14.20. Registro de eventos

La institución dentro su infraestructura cuenta con herramientas que permiten el monitoreo y la gestión de eventos como es a nivel de tráfico en función del origen que permiten conocer ciertos indicadores para la toma de decisiones, entre ellos se tienen:

- FortiGate (Firewall) este dispositivo de seguridad perimetral que ofrece una completa protección de última generación que permite el monitoreo de tráfico tanto interno como externo a través de rutas y

servicios que permiten la comunicación desde y hacia la internet; en su capa de gestión permite bloqueo amenazas basados en indicadores de compromiso permitiendo la contención de la posible amenaza en progreso. Este dispositivo permite recopilar información cuando se estén presentando eventos o incidentes de ciberseguridad, supervisando todo lo que ocurre en la red a través de avisos inmediatos al correo electrónico.

- Consola Antivirus Endpoint, plataforma central que administra la gestión de los clientes que se ejecutan en ordenadores finales y servidores para la protección de anomalías y detección de código malicioso. Permite visualizar el estado de estos, monitorear eventos y realizar despliegue de actualizaciones basado en firmas para la protección de los equipos finales.
- Fortianalyzer permite la visibilidad de la infraestructura y la gestión para eliminar cuellos de botella operativos de tráfico, recopila información histórica y en tiempo real, dando como valor agregado a los equipos de seguridad ser siempre proactivos.
- FortiSIEM, sobre esta plataforma permite la centralización de la información recopilada de diferentes fuentes de dispositivos de red

y de seguridad a través de logs, logrando tomar decisiones tempranas frente anomalías en la actividad real de la infraestructura de la institución.

- Monitoreo continuo del tráfico de los switch Core routers observando el consumo de ancho, estado de paquetes, performance de los appliance.

Estas herramientas nos permiten la identificación temprana de posibles eventos e incidentes de ciberseguridad en los alertamientos de los sistemas para la preparación de la ocurrencia de estos y de esto alistar o preparar los procedimientos necesarios para contener la amenaza en proceso, tal como lo propone la guía (MinTIC, 2021) en la detección, evaluación y análisis de los sistemas.



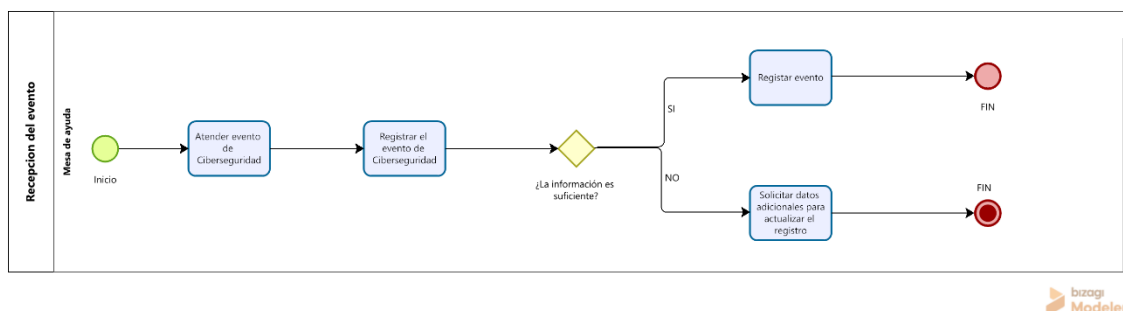
Ilustración 26 Correlación de eventos

Autor: Ramos, Ana (Julio 2021) SIEM, Gestión de eventos e información de seguridad, [ww.mytra.es](https://www.mytra.es/blog-post/siem-gestion-de-eventos-e-informacion-de-seguridad), <https://www.mytra.es/blog-post/siem-gestion-de-eventos-e-informacion-de-seguridad>

El sistema de registro de incidentes permite realizar seguimiento y trazabilidad para la resolución del incidente, este funciona a través del escalamiento o notificación por distintas fuentes de transmisión de la información del incidente por el comportamiento en la detección de la debilidad o vulnerabilidad del sistema afectando la seguridad de la información. (MinTIC, 2021).

Diagrama del registro del evento en el sistema.

Ilustración 27 Subproceso Gestión del evento



Autor: Propio basado a la guía de la NIST SP.800-61r2 Computer Security Incident Handling Guide (NIST, 2020)

14.21. Registro de Incidentes en el Sistema.

El sistema de gestión de incidentes dispone de unos documentos propuestos que permite realizar el seguimiento de cada uno de los procesos, reportes, tareas de control de cada uno y sobre todo las buenas prácticas de documentación sobre las prácticas y acciones realizadas. En este proceso incorpora características relacionadas al incidente como es el control y flujo del tiempo, notificaciones y las responsabilidades en cada uno de los roles de la gestión de incidentes. Así como se establece en la guía (MinTIC, 2021) Declaración y notificación de Incidentes.

Con ayuda de la plataforma GLPI respecto a la gestión de tickets, recopila la información necesaria para almacenar y categorizar el registro de incidentes de forma adecuada; estos registros deben proveen de la información necesaria desde el punto de partida desde que fue registrado el mismo incidente, ya sea en el punto a través de la notificación por correo electrónico, llamada o cualquier otro método de comunicación.

Con base a la guía (NIST, 2023), (MinTIC, 2021)

Como buena práctica de recolección de información, este debe incluir desde el registro la hora y fecha, información necesaria para categorizar la naturaleza del incidente, número del ticket del sistema GLPI, prioridad, urgencia, nombre de la persona quien registra o reporta, descripción de actividades si existieron respecto a la mitigación u acciones realizadas.

La detención del evento que desencadena un incidente es registrada en la plataforma GLPI, esta acción es de obligatorio cumplimiento a nivel interno para cada uno de los miembros de la institución y todo aquel personal que tenga relación de negocio con el ITFIP.

Cada evento que sea reportado de acuerdo con los puntos de notificación y la detección por un empleado y que desencadene o despliegue un incidente de ciberseguridad, será registrado en el sistema GLPI de tickets. En el procedimiento del registro de los incidentes deben ser de estricto cumplimiento a nivel interno o externo siendo miembros de la institución o tengan alguna relación comercial o servicio con el ITFIP. (MinTIC, 2021) Declaración y notificación de incidentes.

Esta directriz de la notificación será socializada y divulgada de acuerdo como lo establece las políticas y lineamientos de seguridad y privacidad de la información, esta directriz define que todo el personal interno como externo de la institución están en la obligación de comunicar las incidencias de seguridad que observen de acuerdo a como se establece en el lineamiento del uso de equipos y tecnologías de información respecto al buen uso del correo electrónico, navegación a internet, gestión de contraseñas, etc.

En estas notificaciones se debe incluir lo siguiente, según como lo recomienda la guía (NIST, 2023) recopilación y manejo de pruebas.

- Fecha y hora del evento o incidente.
- Descripción completa del evento o incidente.
- Activos afectados y tratamientos o datos personales afectados, si aplica.

En la gestión de incidentes, en cada fase y grupo se debe dar un diagnóstico o investigación del posible incidente; desde la primera etapa o fase si la solución no requiere mayor esfuerzo que depende de solo un tipo de solicitud, se debe dar respuesta, resolución, documentación y cierre del ticket rápidamente. Cuando el incidente es de tipo mayor y no es resolutorio en este nivel, deberá ser escalado a un nivel superior, como es la segunda línea de soporte o resolución, grupo de respuesta a incidentes o la gestión de crisis según la criticidad del incidente. (MinTIC, 2021)

Clasificación de incidentes según su identificación:

- Incidentes con prioridad 'baja' o 'normal', la institución toma las acciones correctivas necesarias para la solución del problema, siguiendo el protocolo ordinario de gestión de incidentes.

- Incidentes categorizados con nivel crítico y alto de acuerdo con el impacto que tiene, este tiene un nivel de notificación muy superior que debe ser notificado y comunicado de inmediato, allí se deben tomar todas las acciones correctivas del incidente, integrado al grupo de respuestas a incidentes. Tomado de referencia en la guía (MinTIC, 2021), clasificación de incidentes de seguridad de la información.

14.22. Gestión de equipo de respuesta

El plan de respuesta debe ser detallado y exhaustivo, se proporciona una guía que nos ayuda a categorizar el incidente. Para esto se crea una serie de guías de cómo actuar o responder y los pasos a tomar, involucrando al equipo de gestión de incidentes para responder a un incidente o cuando hay indicios de que podría haberlo.

Las guías para cada uno de los casos son los siguientes.

- Escenario general (Anexo caso general)
- Casos de intrusión (Anexo caso Intrusión)
- Casos de código malicioso (Anexo caso de código malicioso)
- Casos de Phishing (pendiente incluir anexos.)
- Casos de denegación de servicio (Anexo caso de denegación de servicio)

Estas guías son procedimientos detallados para los distintos tipos de incidentes, que inician en su primera fase de Identificación y son un ejemplo para las medidas en la fase de contención y con esto su aplicación a medida no tenga un impacto en la infraestructura y no afecte a la operación del resto de los sistemas.