UNIVERSIDAD NACIONAL DE INGENIERÍA
Facultad de Ciencias y Sistemas

Maestría en Gestión de la Seguridad de la Información

Procedimientos de Gestión de Incidentes de Seguridad de la información, para la División de Informática y Sistemas de la Dirección General de Ingresos de Nicaragua

Monografía para obtener el grado de

Master en Gestión de la Seguridad de la Información

Elaborado por:

Ing. Eddy Onell Cardoza Mendieta

Tutor de Monografía

PhD. Denis Eduardo Hernández García

Managua, Enero 28 del 2020

Dedicatoria

Dedico este trabajo a Jesucristo, Rey de Reyes y Señor de Señores, por darme las fuerzas necesarias para llegar a la meta, a mi niña Jazmín por darme ese beso y ese abrazo cuando ya no podía más y ser el motor que me impulsa, a mi esposa Elizabeth por soportarme tanto, a mi Padre Rafael, por pasarme una taza de café con pan cada vez que estaba frente a la computadora, a todos los que para bien o mal ayudaron que comenzara y terminara este proyecto.

Resumen

En este proyecto, se estableció un manual de procedimientos para la gestión de incidentes de seguridad de la información de la División de Informática y Sistemas de la Dirección General de Ingresos, se realizó una propuesta de roles y responsabilidades del grupo de respuesta a incidentes, se identificaron los incidentes principales y se establecieron formas de reporte y escalamientos. Los involucrados utilizaron este manual como una guía para monitorear los incidentes, estableciendo las mejores prácticas y estándares que involucran medidas o controles de tipo tecnológico, personas y procedimental, que ayudaron a mejorar la atención de incidentes que atentan contra la confidencialidad, integridad y disponibilidad de la información, de riesgos que pueden alterar la operación normal o el logro de los objetivos misionales u organizacionales de la institución.

Las materializaciones de riesgos en tecnologías de la información son conocidos como incidentes de seguridad, que al no tener establecido los procedimientos de gestión de estos, se hace difícil para cualquier institución poderlo identificar, contener y recuperarse de ellos.

Palabras clave: gestión de incidentes, propuestas, procedimientos, seguridad de la información.

Summary

In this project, a manual of procedures for the management of information security incidents of the Information Technology and Systems Division of the Direccion General de Ingresos will be executed, a proposal for roles and commissions of the incident response group was made, The main incidents were identified and report forms and escalations were established. Those involved will use this manual as a guide to monitor incidents, establishing the best practices and methods that involve technological measures or controls, people and procedures, which help to improve the care of incidents that undermine the confidentiality, integrity and availability of the information, of the risks that can alter the normal operation or the achievement of the mission objectives or organizations of the institution.

The materialization of risks in information technologies is known as security incidents, which do not have established the procedures for managing them, it is difficult for any institution to identify, contain and recover them.

Keywords: incident management, proposals, procedures, information security.

Índice

Abreviaciones y acrónimos

DGI	Dirección General de Ingresos
GASI	Grupo de Atención de Servicios Informáticos
DIS	División de Informática y Sistemas
IRT	Equipo de respuestas a incidentes
SGSI	Sistema de Gestión de la Seguridad de la Información
ITIL	Biblioteca de Infraestructura de Tecnologías de la Información
TI	Tecnología de la información
POC	Punto de contacto
SPOC	Simple punto de contacto
CERT	Equipo de respuesta ante emergencias informáticas
CSIRT	Respuesta ante Incidentes de Seguridad de la información
UMOI	Unidad de monitoreo informático
HTTP	Protocolo de transferencia de hipertextos
IPS	Sistema de prevención de intrusiones
APT	Amenaza persistente avanzada
DDoS	Denegación de servicio distribuido
SIAEX	Sistema de administración de exoneraciones
MTTR	Tiempo medio de recuperación

I. Introducción

Los constantes avances en el uso de las tecnologías de la información y las comunicaciones han llevado a las instituciones gubernamentales de Nicaragua como la Dirección General Ingresos de Nicaragua a prepararse para afrontar los riesgos de seguridad a los que puede estar expuesta su información. La información es uno de los activos que ha tomado mayor relevancia en las instituciones del gobierno, lo cual conlleva a implementar procedimientos y acciones que ayudan asegurar la información, como una forma de responder a los incidentes que la afecten.

En la mayoría de los casos, así como dentro de la División de informática y sistemas de la Dirección General de Ingresos el impacto de estos incidentes se ve reflejado en la confidencialidad como por ejemplo: robo de información, en la integridad, relacionada con alteración de información, y en la disponibilidad, teniendo en cuenta que puede causar que los servicios tecnológicos o de información de la Dirección General de Ingresos no estén disponibles, lo cual puede causar pérdidas en la recaudación de los impuestos del país, de relaciones de confianza por los contribuyentes, que conllevarían también a la pérdida de imagen de la Dirección General de Ingresos.

En este proyecto se muestra una propuesta de los Procedimientos de Gestión de Incidentes de la Seguridad de la información para la División de informática y Sistemas de la Dirección General de Ingresos, aunque esta división tenga procedimientos de primera instancia, no se toman medidas para identificar, evaluar y gestionar con eficacia los incidentes tomando en cuenta principios estandarizados y aplicando las buenas prácticas que ayuden a restaurar la funcionalidad normal de los servicios.

Podrá tener la institución recaudadora herramientas que ayudarán a gestionar los incidentes, pero estas herramientas no podrán de alguna manera distinguir entre un incidente principal de uno, que no lo es, ni cuenta con un equipo (IRT) de gestión de incidencias. Las herramientas es el último de los parámetros que debe tener en cuenta, lo primero que hay que considerar son las personas y los procesos establecidos, también la base para la restauración de los sistemas, ningún sistema de incidentes resolverá nada, eso lo tendrá que hacer un equipo, estableciendo normas perfectamente estructuradas propias de la institución.

Se aplicarán algunos principios del estándar internacional ISO / IEC27035-3 que proporciona una guía sobre la operación práctica y las pautas de respuesta para tomar medidas contra la evolución de incidentes que básicamente están orientadas a la detección, evaluación, reporte, decisión, confirmación, respuesta y equipo de respuesta a incidentes, tomando en cuenta la mesa de ayuda establecido en la División de informática y sistemas llamado **Grupo de Atención de Servicios**

informáticos (GASI), como base primera de monitoreo para que pueda ser integrado en el proceso de gestión de incidentes.

El proyecto está orientado al análisis de prácticas de gestión de incidentes seguridad de la información extrayendo los puntos más relevantes para ser integrarlos y posteriormente los procedimientos para responder ante incidentes de seguridad de la información.

Se analizará la situación actual, así como los mecanismos existentes que monitorean los incidentes, también se propone un manual de procedimientos en gestión de incidentes de seguridad para la División de informática y sistemas.

En esta investigación se desarrollaran únicamente los aspectos relacionados directamente con el propósito del proyecto.

II. Antecedentes y Planteamiento del problema

La División de informática y sistemas de la Dirección General de Ingresos, tiene implementado controles de sistema de gestión de seguridad de la información (SGSI) basado en la ISO 27001:2013, así como también un servicio de mesa de ayuda basado en las buenas prácticas desarrolladas por ITIL, aplicadas por la mesa de ayuda, **Grupo de Atención de Servicio informáticos (GASI).**

La problemática en la institución es que no se aplica la gestión de incidentes de seguridad de la información, principalmente en el área de la División de informática y Sistemas. Es necesario diseñar este manual de procedimientos como herramienta para la oficina de seguridad de la información, responsables de áreas, analistas, así como para cargos superiores. Por lo tanto, este manual dispondrá de herramientas para ayudar a desarrollar normas con el fin de reportar y gestionar la información de todos los incidentes, incluso aquellos que suceden más a menudo y que, por lo general, no se considerarían críticos.

Los enfoques actuales están diseñados en base a ciertos procedimientos de primera instancia, que abarcan algunos aspectos, pero no representan un enfoque general de evaluar, contener y resolver, dentro de ellos reporte, decisión confirmación, respuesta y equipo de respuesta, basada en la gestión de incidentes de seguridad de la información.

No se lleva un registro, ni se posee una base del conocimiento, ni una documentación centralizada para evitar recurrencia de los eventos de seguridad de la información. Los usuarios no son capacitados no se les proporcionan fuentes de información actualizadas que logren una mejor respuesta en el caso de un incidente mayor.

Los procedimientos de gestión de incidentes requieren de la aprobación del director de informática y la autorización del Director General de Ingresos para su implementación en el área organizativa de la Seguridad de la Información.

III. Justificación

La realización de los procedimientos de gestión de incidentes de seguridad de la información basado en buenas prácticas de gestión de seguridad y embebido dentro de los servicios de gestión de eventos e incidentes, son importantes para atender adecuadamente las siguientes necesidades y beneficios comunes para la División de informática y sistemas de la Dirección General de Ingresos:

• Identificación de la mayoría de los eventos e incidentes concernientes a la seguridad de la información.

• Mayor oportunidad en la identificación, atención y respuesta de los incidentes de seguridad de la información.

• Centralización y optimización de recursos para la gestión de todos los eventos e incidentes que se presentan.

• Registro centralizado para la documentación de seguridad para evitar la recurrencia de los incidentes.

• Disposición y uso de una de las fuentes de información más importante para la identificación y el análisis de los riesgos de seguridad de la información como lo es la gestión de incidentes de seguridad.

• Servir como un recurso confiable para analizar la efectividad de los controles de seguridad de un sistema de gestión de seguridad de la información basado en algunos principios del estándar ISO/IEC 27035-3.

IV. Objetivos

a. General

Proponer un manual de Procedimientos de Gestión de Incidentes de Seguridad de la Información para la División de informática y Sistemas de la Dirección General de Ingresos de Nicaragua, que permita una mejor respuesta en la gestión ante estos incidentes de seguridad, sin detener las operaciones o servicios que la institución ofrece.

b. Específicos

- Definir los roles y responsabilidades dentro de la División de Informática y sistemas de la Dirección General de Ingresos en cuanto a incidentes de la seguridad de la información.
- Identificar los incidentes de la seguridad de la información para ser evaluados.
- Definir los procedimientos formales de reporte y escalada de los incidentes de seguridad de la información.
- Definir los mecanismos que permitan monitorear los tipos de incidentes de seguridad de la información a través de una base de conocimiento y registro de los incidentes.
- Definir estrategias o procedimientos de solución a los diferentes tipos de incidentes tomando en cuenta las mejores prácticas y estándares.

V. Marco teórico

La gestión de incidentes de seguridad de la información es una de esas acciones (controles tecnológicos, capacitaciones, análisis de riesgos, entre otros) que se deben implementar para asegurar y proteger la información de las empresas o entidades, a través de este documento se presentará los procedimientos de gestión de incidentes de seguridad.

Un Incidente se define como cualquier anomalía que suponga la destrucción, perdida o alteración accidental o ilícita de datos de carácter personal transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

Evento de seguridad de la información

Ocurrencia identificada de un sistema, servicio o estado de la red que indica un posible incumplimiento de la seguridad de la información, la política o la falla de los controles, o una situación desconocida que puede ser relevante para la seguridad.

"En el caso de las herramientas de gestión de eventos de seguridad, su principal función es ayudar a la solución de incidentes de seguridad, para ello emiten alertas y notificaciones para investigar los eventos más importantes". (Ramos, 2014).

Incidente mayor

Un incidente que causa un impacto significativo en el negocio, cuya urgencia requiere más tiempo para resolverlo que un incidente normal, y afecta a numerosos usuarios.

"Las personas a veces confunden un incidente importante con un problema, sin embargo, un incidente siempre sigue siendo un incidente, su impacto o prioridad puede aumentar, pero nunca se convierte en un problema". (Bernard, 2014).

Gestión de incidentes de seguridad de la información

Procesos para detectar, informar, evaluar, responder, tratar y aprender de incidentes de seguridad de la información.

La gestión de incidentes tiene como objetivo calcular y utilizar adecuadamente los recursos necesarios para aplicar correctamente estas medidas de prevención, detección y corrección de incidentes de seguridad. (Tejada, 2015).

Manejo de incidentes

Acciones de detección, informe, evaluación, respuesta, tratamiento y aprendizaje de incidentes de seguridad de la información.

Cuando un evento cibernético interrumpe las operaciones de TI, es esencial restaurar el servicio a su funcionamiento normal lo más rápido posible; este es el propósito de la gestión de incidentes. (Schreider, 2017).

Respuesta al incidente

Acciones tomadas para proteger y restaurar las condiciones operativas normales de un sistema de información y la información almacenada en él cuando ocurre un incidente de seguridad de la información.

La respuesta a incidentes es un deporte de equipo, y no deja espacio para el ego, la actitud o la falta de confianza dentro del equipo. Es importante responsabilizar a las personas, pero es injusto si son responsables sin haber sido capacitadas o informadas sobre las expectativas de la empresa. (Schnepp, Vidal y Hawley, 2017. P.11).

Punto de contacto (PoC)

Identificación de medios de comunicación como, persona (s) y organización (es) asociados con el (los) recurso (s). Un POC (también punto de contacto único o SPOC) puede ser una persona o un departamento que actúa como coordinador o punto focal de información sobre una actividad o programa. Los POC se utilizan en muchos casos donde la información es sensible al tiempo y la precisión es importante.

Equipos de respuesta a incidentes (IRT).

Un equipo de miembros de la organización debidamente capacitados y de confianza que manejan los incidentes durante su ciclo de vida.

El IRT como se describe en esta Norma Internacional es una función organizativa que cubre el proceso de incidentes de seguridad de la información y se centra en incidentes relacionados con TI. Otras funciones comunes (con abreviaturas similares) dentro del manejo del incidente pueden tener un alcance y propósito ligeramente diferentes. Las siguientes son abreviaturas de uso común, aunque no son exactamente las mismas:

- CERT®: un equipo de respuesta ante emergencias informáticas se centra en la tecnología de la información y las comunicaciones.
- CSIRT: un equipo de respuesta a incidentes de seguridad informática es una organización de servicio que se encarga de recibir, revisar y responder a los informes y la actividad de incidentes de seguridad informática. Estos servicios generalmente se realizan para una circunscripción definida, que podría ser una entidad matriz como una corporación, organización

gubernamental u organización educativa; una región o país; una red de investigación; o un cliente pagado.

Miembros del equipo a tiempo completo versus a tiempo parcial: la mayoría de las entidades no tienen empleados a tiempo completo dedicados a la respuesta a incidentes. El equipo de respuesta generalmente está formado por miembros que tienen otras responsabilidades. La idea es que, si ocurre un incidente, se adopte un enfoque práctico. (Thompson, 2018).

Fases de la gestión de incidencias

a. **Detección y reportes**

Los eventos de seguridad de la información pueden ser detectados directamente por una persona o personas que notan algo que es motivo de preocupación, ya sea técnico, físico o relacionado con el procedimiento. Una capacidad efectiva de respuesta a incidentes requiere la participación de varias personas dentro de la organización. Tomar las decisiones correctas de planificación e implementación es clave para establecer un programa exitoso de respuesta a incidentes. (Stallings, 2018).

b. **Informe de eventos**

Cualquiera que sea la fuente de la detección de un evento de seguridad de la información, la persona notificada por medios automáticos, o notando directamente algo inusual, es responsable de iniciar el proceso de detección e informe. Esta podría ser cualquier miembro del personal de una organización, ya sea personal permanente o contratado. La persona debe seguir los procedimientos y utilizar el formulario de informe de eventos de seguridad de la información especificado por el esquema de administración de incidentes de seguridad de la información.

c. **Evaluación y decisión inicial del PoC**

El PoC debe realizar una evaluación para determinar si el evento de seguridad de la información debe clasificarse como un incidente de seguridad de la información o si de hecho es una falsa alarma (incluso mediante el uso de la escala de clasificación de incidentes acordada por la organización).

d. **Evaluación y confirmación de incidencias por el IRT (Equipo de respuesta a incidentes.**

La evaluación, y la confirmación de la decisión sobre si un evento de seguridad de la información se debe clasificar como un incidente de seguridad de la información, debe ser responsabilidad del IRT. Si aún existe cierto grado de incertidumbre en cuanto a la autenticidad del incidente de seguridad de la

información o la integridad de la información reportada, el miembro del IRT debe realizar una evaluación para determinar si el incidente de seguridad de la información es real o de hecho es una falsa alarma. Esta división se asegurará de que las políticas, planes y estándares de ciberseguridad se formulen, implementen, supervisen y evalúen. (DICT Computer Emergency Response Team (CERT) Manual).

e. Respuestas inmediatas

Las siguientes actividades para el miembro del IRT son identificar las acciones de respuesta inmediata para tratar el incidente de seguridad de la información, registrar los detalles en el formulario del incidente de seguridad de la información y dentro de la base de datos de incidentes / vulnerabilidades / eventos de seguridad de la información, y notificar a Las acciones requeridas a las personas o grupos apropiados.

f. Actualización de la información del incidente

Cualquiera que sea el próximo paso que se determine, el miembro de IRT debe actualizar el informe de incidentes de seguridad de la información tanto como sea posible, agregarlo a la base de datos de incidentes / vulnerabilidades de seguridad de la información y notificar al administrador de IRT y a otros según sea necesario. (ISO IEC 27035-3, 2017)

g. Evaluación del control sobre incidentes de seguridad de la información

Después de que el miembro del IRT haya instigado las respuestas inmediatas y las actividades relevantes de análisis. Se debe determinar rápidamente si el incidente de seguridad de la información está bajo control. Si se confirma que el incidente de seguridad de la información está bajo control, el miembro del IRT debe instituir cualquier respuesta posterior requerida, para finalizar el incidente de seguridad de la información y restaurar el sistema de información afectado a las operaciones normales. Si se confirma que el incidente de seguridad de la información no está bajo control, entonces el miembro del IRT debe iniciar actividades de crisis.

h. Respuestas posteriores

Después de haber determinado que un incidente de seguridad de la información está bajo control y no está sujeto a actividades de crisis, el miembro del IRT debe identificar si y qué respuestas adicionales se requieren para lidiar con el incidente de seguridad de la información. Esto podría incluir restaurar el (los) sistema (s) de información, servicio (s) y / o red (es) afectado (s) a su funcionamiento normal.

Luego, debe registrar los detalles en el formulario de informe de incidentes de seguridad de la información y en la base de datos de incidentes / vulnerabilidades / eventos de seguridad de la información, y notificar a los responsables de completar las acciones relacionadas. (ISO IEC 27035-3, 2017).

i. Respuestas a situaciones de crisis

Las mejores opciones para tratar todos los tipos posibles de incidentes de seguridad de la información que podrían afectar la disponibilidad y, hasta cierto punto, la integridad de un sistema de información, deberían haberse identificado en el plan de gestión de crisis de la organización. Estas opciones deben estar directamente relacionadas con las prioridades comerciales de la organización y los plazos relacionados con la recuperación y, por lo tanto, con los períodos de interrupción máximos aceptables para TI, voz, personas y alojamiento.

Al establecer mecanismos sólidos de gestión de crisis, usted puede optimizar la preparación y reducir el riesgo de que ocurra un incidente, o disminuir su impacto. (Managing the message: Communication and media management in a security crisis, 2013).

j. Comunicaciones

En muchos casos, cuando el IRT ha confirmado que un incidente de seguridad de la información es real, es necesario que ciertas personas estén informadas tanto internamente (fuera de las líneas normales de comunicación de IRT / gestión) como externamente, incluida la prensa. Es posible que esto deba ocurrir en varias etapas, por ejemplo, cuando un incidente de seguridad de la información se confirma como real, cuando se confirma como bajo control, cuando se designa para actividades de crisis, cuando se cierra y cuando se realiza la revisión posterior al incidente. Completado y conclusiones alcanzadas.

El Plan de Respuesta a Incidentes tiene que contemplar cómo la organización debería comunicar a terceros la causa y las posibles consecuencias de un incidente de seguridad informática. (Gómez, 2011).

k. Escalada

En circunstancias extremas, es posible que haya que escalar los asuntos para adaptarse a incidentes que están fuera de control y un peligro potencial de impacto comercial inaceptable. Es necesario escalar estos incidentes para activar el plan de continuidad del negocio si se implementa informando a la alta gerencia, a otro grupo dentro de la organización o a personas o grupos fuera de la organización.

l. Registro de actividad y control de cambios.

Se enfatiza que todos los involucrados en el informe y la gestión de un incidente de seguridad de la información deben registrar correctamente todas las actividades

para su posterior análisis. Esta información debe conservarse de forma segura y con un régimen de respaldo adecuado.

Establecimiento de los Equipos de Respuesta a Incidentes (IRT)

Los IRT son equipos de miembros de la organización debidamente capacitados y de confianza que brindan respuestas, análisis y prevenciones adecuadas de diversos incidentes que ocurren en las redes de computadoras.

Tipos de los IRT

En general, los IRT se pueden clasificar en tres tipos diferentes: únicos, jerárquicos y remotos según el objetivo deseado de las organizaciones. (ISO IEC 27035-3, 2017).

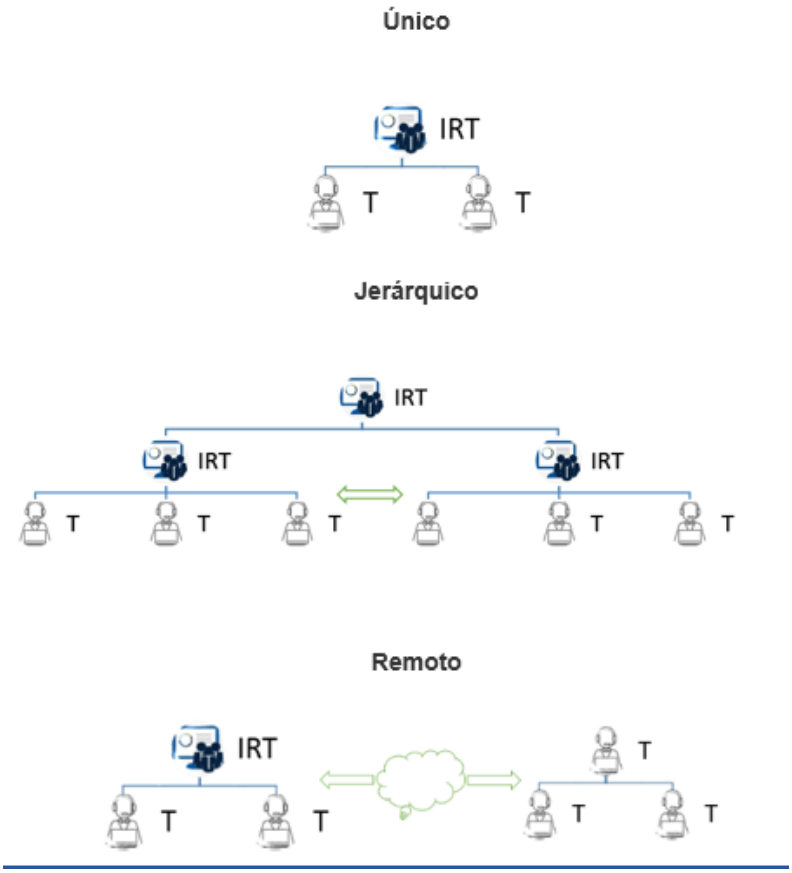


Fig.1. Tipos de IRT (Fuente ISO 27035-3)

Roles de los IRT

Para proporcionar una respuesta rápida a varias amenazas, los IRT requieren una política de respuesta, procedimientos de respuesta y actividades de operación. Las principales funciones de los IRT son las siguientes:

- Gestión de sistemas de seguridad integrados.
- Implementar una política consistente.
- Responder rápidamente.
- Operar la estructura de seguridad optimizada.

Si se toma la decisión de proporcionar las capacidades de respuesta a incidentes a través de un equipo interno, el siguiente hito importante es identificar los roles que se incluirán en el equipo y los conjuntos de habilidades requeridos para esos roles. (Lucas y Moeller, 2004).

Organización IRT

Las políticas de prevención y respuesta rápidas deben establecerse teniendo en cuenta los puntos de vista físicos, técnicos y administrativos. Los IRT deben registrar, manejar y prevenir incidentes con las actividades adecuadas de forma rápida y precisa.

Habilidades y calificaciones del personal

Los IRT se pueden estructurar de manera diferente según el tamaño de la organización, su personal y el tipo de industria. Las respuestas a incidentes generalmente dependen de la capacidad y confiabilidad del personal en IRT.

El personal de IRT y sus capacidades se vuelven especialmente más importantes porque las actividades de los IRT incluyen establecer la política de seguridad para prevenir incidentes, auditar, coordinar con otros departamentos y actividades técnicas.

Habilidades de equipo: los miembros del personal de CSIRT deben ser flexibles en sus métodos de trabajo como jugadores de equipo productivos y cordiales. Se requiere que los miembros del personal de CSIRT sean conscientes de sus responsabilidades, contribuyan a los objetivos del equipo y trabajen juntos para compartir información y carga de trabajo. (EC-Council, 2016).

VI. Análisis y presentación de resultados

Capítulo 1. Análisis de Gestión de incidentes de seguridad de la información actual en la División de Informática y sistemas de la DGI.

1.1 Roles y responsabilidades dentro de la División de informática y sistemas actuales.

La Misión de la División de informática y Sistemas de la DGI.

Asegurar el diseño, desarrollo, implantación, configuración y funcionamiento de los sistemas informáticos, operativos, bases de datos, redes, telecomunicaciones, equipos y prestación de servicios requeridos por las máxima autoridad y áreas requirentes, a fin de garantizar un servicio efectivo de apoyo informático a todos los niveles de la Dirección General de Ingresos.

La División de Informática y Sistemas es un área de apoyo que depende de la Dirección Superior. La Disposición Administrativa Interna No. 02-2016, en las actividades de control establece: Procedimientos separados para cada unidad organizativa, se identifican riesgos operativos de los diferentes procedimientos que se ejecutan en la DIS (División de informática y sistemas) y los formatos que se utilizan en la operatividad de dicha división.

Las funciones generales de la DIS se pueden definir en:

1. Organizar, dirigir y controlar los servicios y sistemas automatizados de acuerdo a las leyes, reglamentos y disposiciones de la institución.
2. Diseñar, definir y elaborar los programas y normas que regulen el ordenamiento informático en la institución.
3. Recomendar, proponer e implantar nuevas aplicaciones tecnológicas en software y hardware, para mejorar los sistemas de información, equipos, normas y procedimientos de desarrollo, instalación, mantenimiento, operación y producción.
4. Ser miembro de la comisión en los procesos de licitación de los equipos y soportes técnicos y la elaboración de los presupuestos de inversión de tecnología a adquirirse, así como definir los requisitos que deben reunir la plataforma informática y el personal profesional que intervendrá en su desarrollo.
5. Administrar el mantenimiento preventivo y correctivo de toda la infraestructura informática, a fin de garantizar el funcionamiento de los sistemas automáticos y administrativos de la institución.

6. Apoyar los programas de análisis de informaciones económicas-fiscales, para la administración tributaria, generando base de datos en herramientas y aplicaciones para obtener información estadística interna y externa a la institución.
7. Informar mensualmente a la División de Planificación Estratégica del avance en las acciones del Plan Operativo Anual (POA) del Área, así como los insumos para la Evaluación del POA y otras tareas propias de esta Unidad Administrativa.
8. Informar mensual y periódicamente de las actividades y cambios en los sistemas de información gerencial, de control de gestión, administrativos y tributarios de la institución.
9. Apoyar plenamente la reforma de la DGI y el logro de los objetivos para el cambio tal como se definiera en el Plan Estratégico aprobado.
10. Evaluar anualmente el desempeño laboral del personal subalterno y remitir resultados a través de Acta, a la División de Recursos Humanos.
11. Las demás funciones que le asigne la Dirección Superior.

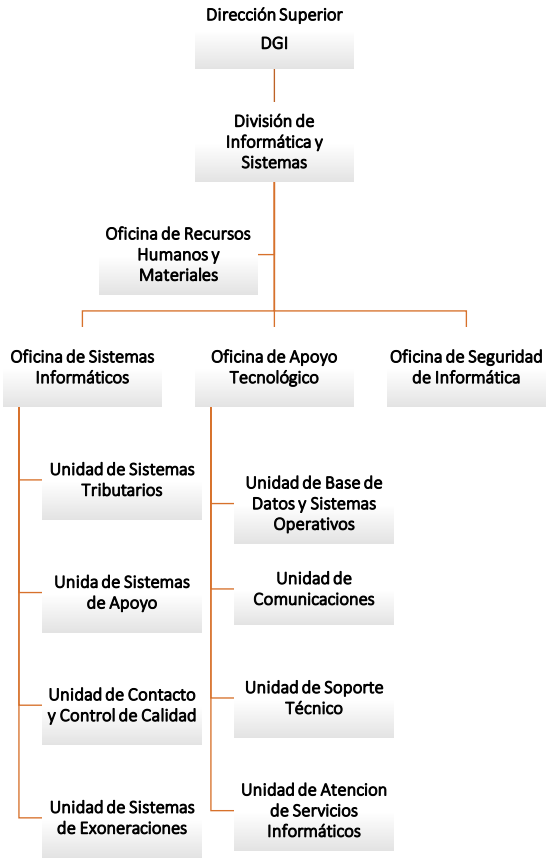


Fig. 2 Estructura organizacional de la División de informática y sistemas

(Fuente www.dgi.gob.ni)

A continuación se detallan las funciones según el organigrama:

- **Director de informática y sistemas**: Planificar, dirigir, coordinar y dar seguimiento al diagnóstico, desarrollo e implementación de las tecnologías de información y comunicación en los sistemas de información tributarios de la Institución, así mismo elaborar, implantar y controlar la aplicación de tecnologías de comunicación, normas, políticas de seguridad a nivel institucional y velar por la administración y funcionamiento de la red informática instalada y el mantenimiento preventivo y correctivo de los equipos informáticos de la Dirección General de Ingresos, de acuerdo a las necesidades de modernización institucional, leyes, normativas, procedimientos establecidos y orientaciones de la Dirección Superior, a fin de contribuir al logro de los objetivos y metas institucionales, a través de la sistematización, optimización y automatización de los procesos de trabajo y de servicios a los contribuyentes por medio de las tecnologías de información y comunicación.
- **Subdirector de informática y sistemas:** Coordinar e implantar el funcionamiento, administración y mantenimiento de los sistemas de información automatizados y al sistema de información tributaria en la Dirección General de Ingresos así como elaborar la documentación técnica de los sistemas y de los manuales de usuarios de los mismos.
- **Jefe(a) de oficina de sistemas informáticos:** Planificar y dar seguimiento a la ejecución de planes informáticos de desarrollo de sistemas de información automatizados para la Institución, así mismo participar en la elaboración de estándares para el análisis, diseño y desarrollo de sistemas, de conformidad a las solicitudes presentadas por los usuarios, leyes, normas, procedimientos establecidos e instrucciones del Superior Inmediato, a fin de facilitar los procesos de trabajo y contribuir a la modernización de la gestión Institucional.
    - **Jefe(a) Unidad de Sistemas Informáticos Tributarios**: Coordinar, revisar, elaborar y participar en los procesos de desarrollo, instalación de las bases de datos en el servidor, migración y mantenimiento de los Sistemas de Información Tributaria, así como asistir técnicamente a los usuarios directos sobre el uso y manejo apropiado de los mismos, de acuerdo a normas, procedimientos vigentes e instrucciones del Superior Inmediato, a fin de garantizar la agilización de los procesos de trabajo de los diferentes Sistemas Tributarios, orientados a la actualización tecnológica de la Dirección General de Ingresos.

- **Jefe(a) Unidad Sistemas de Apoyo Informático**: Coordinar, supervisar y realizar actividades de desarrollo y mantenimiento de sistemas de Información Automatizados y elaboración de normativas relacionadas, así mismo coordinar y brindar asistencia técnica a usuarios de la institución en materia de sistemas, de acuerdo a normas, procedimientos establecidos e instrucciones del Superior Inmediato, a fin de garantizar el procesamiento y difusión de información generada en las distintas áreas de la Dirección General de Ingresos.
- **Jefe(a) Unidad de Contacto y Control de Calidad**: Planificar, Coordinar, Supervisar y dar seguimiento al desarrollo de nuevos software de calidad; diagnosticar problemas encontrados en el sistema y cumplir con la corrección de los mismos mediante la ejecución de mecanismos informáticos de prueba y control de calidad, de conformidad a normas, procedimientos establecidos, Código Tributario, Ley de Equidad Fisca y directrices del superior inmediato, con el objetivo de asegurar a los usuarios calidad y eficiencia de los Software desarrollados y el soporte técnico de los mismos.
- **Jefe(a) Unidad de Sistemas de Exoneraciones**: Coordinar, revisar, elaborar y participar en los procesos de desarrollo de nuevos requerimientos funcionales del Sistema de Administración de las Exoneraciones (SIAEX), instalación de base de datos en el servidor, migración de archivos y mantenimiento del sistema, así como asistir técnicamente a los usuarios directos sobre el uso y manejo correcto de las diferentes aplicaciones del sistema, de acuerdo a normas, procedimientos vigentes e instrucciones del superior inmediato a fin de garantizar la agilización de los procesos de trabajo orientados a la actualización tecnológica de la Dirección General de Ingresos.

- **Jefe(a) Oficina de Apoyo Tecnológico:** Coordinar, controlar y dar seguimiento al diseño, desarrollo, implementación y funcionamiento de los sistemas automatizados, base de datos, red y telecomunicación de la Dirección General de Ingresos, así como al mantenimiento preventivo y correctivo de los equipos informáticos existentes y presentar propuesta del plan de adquisición de nuevos equipos y software actualizados, de conformidad a normas técnicas, procedimientos establecidos e instrucciones del Superior Inmediato, con el fin de asegurar la automatización efectiva de los procesos de trabajo desarrollados en la Institución y el óptimo funcionamiento de los equipos informáticos.

- **Jefe(a) Unidad Base de Datos y Sistemas Operativos**: Coordinar y supervisar el desarrollo, implementación, mantenimiento, resguardo y seguridad de Sistemas de Información de la Dirección General de Ingresos, su funcionamiento relativo a la administración, recolección, actualización, normalización de datos, de acuerdo a mecanismos y metodologías aplicadas a la administración de sistemas fiscales interinstitucional y regional e instrucciones del Superior Inmediato, con el fin de garantizar información actualizadas que faciliten los diferentes procesos de trabajo, que se desarrollan en la Institución.
- **Jefe(a) Unidad de Comunicaciones**: Formular e implementar estrategias de desarrollo físico y lógico de la red de comunicación Institucional; administrar y controlar los recursos tecnológicos y efectuar el mantenimiento preventivo y/o correctivo, de conformidad a normativas, procedimientos, estándares de calidad establecidos y orientaciones del Superior Inmediato, a fin de asegurar el flujo e intercambio efectivo de información generada en la Dirección General de Ingresos.
- **Jefe(a) Unidad de Soporte Técnico:** Programar, coordinar y dar seguimiento al buen funcionamiento de los equipos informáticos de la Dirección General de Ingresos, para un mejor aprovechamiento de los recursos informáticos, de conformidad a normas y procedimientos establecidos e instrucción del Superior Inmediato, a fin de asegurar la comunicación tecnológica institucional.
- **Jefe(a) Unidad Grupo de Atención de Servicios Informáticos**: Coordinar las consultas atendidas por los Analistas de la Unidad del Grupo de Atención de Servicios Informáticos, analizar y clasificar los tipos de solicitudes, así mismo gestionar antes las Unidades Tecnológicas las solicitudes presentadas, de acuerdo a normas y procedimientos a fin de garantizar la eficiencia, optimizando tiempo y recursos informáticos.

- **Jefe(a) Oficina de Seguridad Informática**: Planificar, organizar, dirigir, coordinar y controlar las acciones que conlleven a una implementación exitosa de la seguridad informática de servicios y/o recursos de tecnologías de información que soporten la operatividad de la institución de conformidad con las leyes, normas, procedimientos establecidos e

instrucciones del superior inmediato a fin de facilitar los procesos de trabajo y contribuir al fortalecimiento de la gestión institucional.

1.2 Diagnóstico de la situación actual.

La Seguridad de la Información se gestiona a través de la aprobación de normativas internas **DAI-08-2011: Plan de acciones inmediatas para garantizar la seguridad de la información.** Sin embargo, como parte de la estandarización de los procesos se adopta un marco de trabajo basado en la ISO/IEC 27001: Requisitos para Sistemas de Gestión de la Seguridad de la Información.

También se gestiona a través de la normativa interna **DAI-12-2011: Comité para investigación control y sanción de los casos relacionados con el abuso o manipulación de la información institucional.** En el cual se procede a sancionar administrativamente al o los usuarios en el caso encontrar responsabilidad en los casos investigados.

Actualmente se está implementando la oficina de seguridad informática, los procedimientos actuales en el manejo de incidentes de seguridad de la información carecen de un manual de procedimientos en el caso que se produzcan incidentes de seguridad de la información o un incidente. Así como la unidad de monitoreo informático (**UMOI**), el cual monitorea los diversos servicios críticos de la **DIS** 24/7.

La gestión de servicios para división de informática y sistemas y DGI los ofrece la mesa de ayuda **(GASI).** El cual actúa como primera unidad en determinar los niveles de incidentes de seguridad de la información antes de pasar a un incidente mayor.

Con el propósito de conocer más sobre la situación actual en gestión de incidentes, se les realizó una encuesta a los directores DIS pero no nos proporcionaron la información solicitada (ver anexo 11).

A continuación se detallan los servicios críticos de la DIS, llámese servicios críticos a aquellos que pueden generar retraso o pueden causar pérdidas en la recaudación de tributos.

1. Servicios de redes centrales:
    a. DNS (Linux,) DHCP (Windows servers 2019)
    b. Cortafuegos de centro / centro de datos: IPS: McAfee https://10.16.221.711/intruvert/jsp/module/Login.jsp
    c. Equilibrador de carga web: https://f5.com/es/products/big-ip
2. Centro de datos:
    a. Servidores: IPS, ATENEO, SIIAF, CORREO, ERUC, NAGIOS, CATASTRO EN LINEA, EXONERACIONES, SACFI, DGI EN LINEA
    b. UPS: CNDF 1, CNDF2, SYMETRA
    c. Unidades precisión: unidad de precisión 1, 2, 3.

    d. Virtualización: (Openfiler) (todos).
3. Correo electrónico: https://mail.dgi.gob.ni/?loginOp=logout
4. Sitios web
    a. https://dgienlinea.dgi.gob.ni/
    b. https://catastro.dgi.gob.ni/Cuenta/Index?ReturnUrl=%2F
    c. www.dgi.gob.ni
5. Sistema telefónico: https://www.issabel.org/
6. Oracle Financials: Sorgensys y Gensys
7. Sistemas físicos de acceso a puertas: https://www.zktecolatinoamerica.com/

Capítulo 2. Mecanismos que permiten monitorear los incidentes de seguridad de la información de la DGI.

En este capítulo se describen diferentes sistemas y unidades que monitorean los diferentes incidentes de seguridad de la información, se hará una propuesta de estructura organizacional de Gestión de Incidentes, se identificaran los principales incidentes en sus etapas, niveles de prioridad y acciones recomendadas.

- **Unidad de monitoreo informático (UMOI)**: este grupo de monitoreo 24/7 está encargado de alertar cualquier evento que se produzca en toda la infraestructura y servicios que presta la DGI en la División de informática y sistemas**.** El grupo actúa como un equipo de alerta, el cual informa y notifica los eventos ocurridos durante 24 horas.

  Sistemas actuales que se utilizan como base en el monitoreo de incidentes.

  - NAGIOS: permite monitorear virtualmente todas las aplicaciones, servicios internos y externos de la DIS. http://nagios.dgi.gob.ni/nagios
  - DLP: Protección de perdida de datos. https://www.mcafee.com/enterprise/en-hk/products/dlp-endpoint.html#
  - PRTG Monitor de redes: Supervisa todos los sistemas, dispositivos, tráfico y aplicaciones de la infraestructura de la DIS.
  - Consola Eset Endpoint Antivius 7.
  - Sistema de cámaras de seguridad.
  - Control de acceso a puertas DIS: software profesional de control de acceso. https://www.zktecolatinoamerica.com/

- **Grupo de atención de servicios informáticos (GASI):** punto único de contacto para los diferentes servicios que los usuarios solicitan, en el cual se determinan algunos incidentes de seguridad, el usuario reporta vía correo, telefónico o mensajería, con servicio web aplicativo http://servicios.dis.dgi.gob.ni

2.1 Propuesta de estructura organizacional de gestión de incidentes.

Se crearan los cargos de coordinador, administrador y líder de incidentes, grupo técnico (GASI, UMOI) con sus responsabilidades y procesos en el caso de un incidente mayor, los cual permitirá al grupo de respuesta a incidentes 24/7 minimizar el tiempo en la restauración de uno o los servicios que la DIS ofrece a los contribuyentes de la Dirección General de Ingresos.

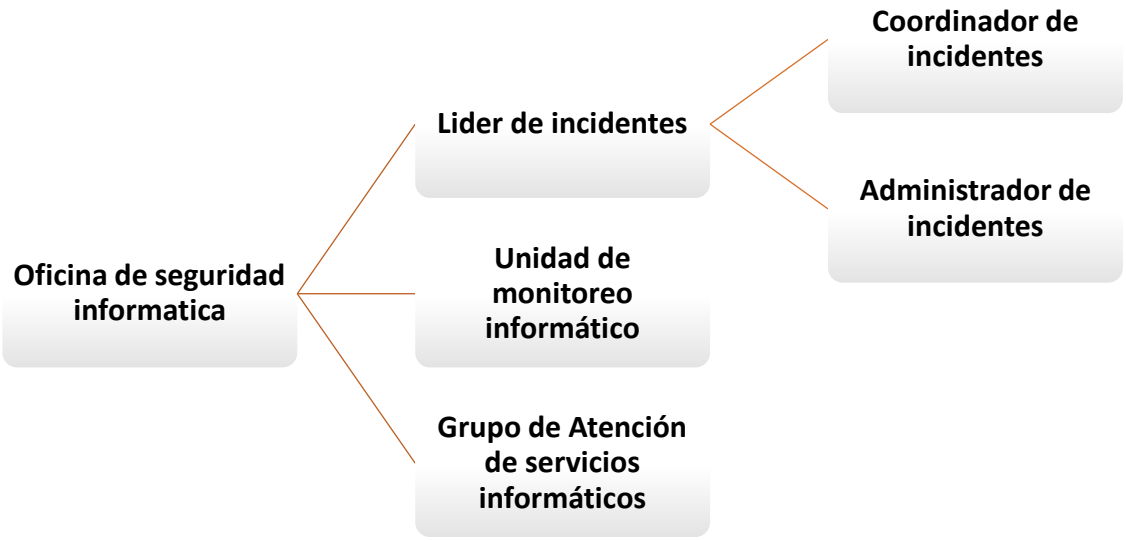


Fig. 3 Propuesta de estructura organizacional de Gestión de incidentes DIS.

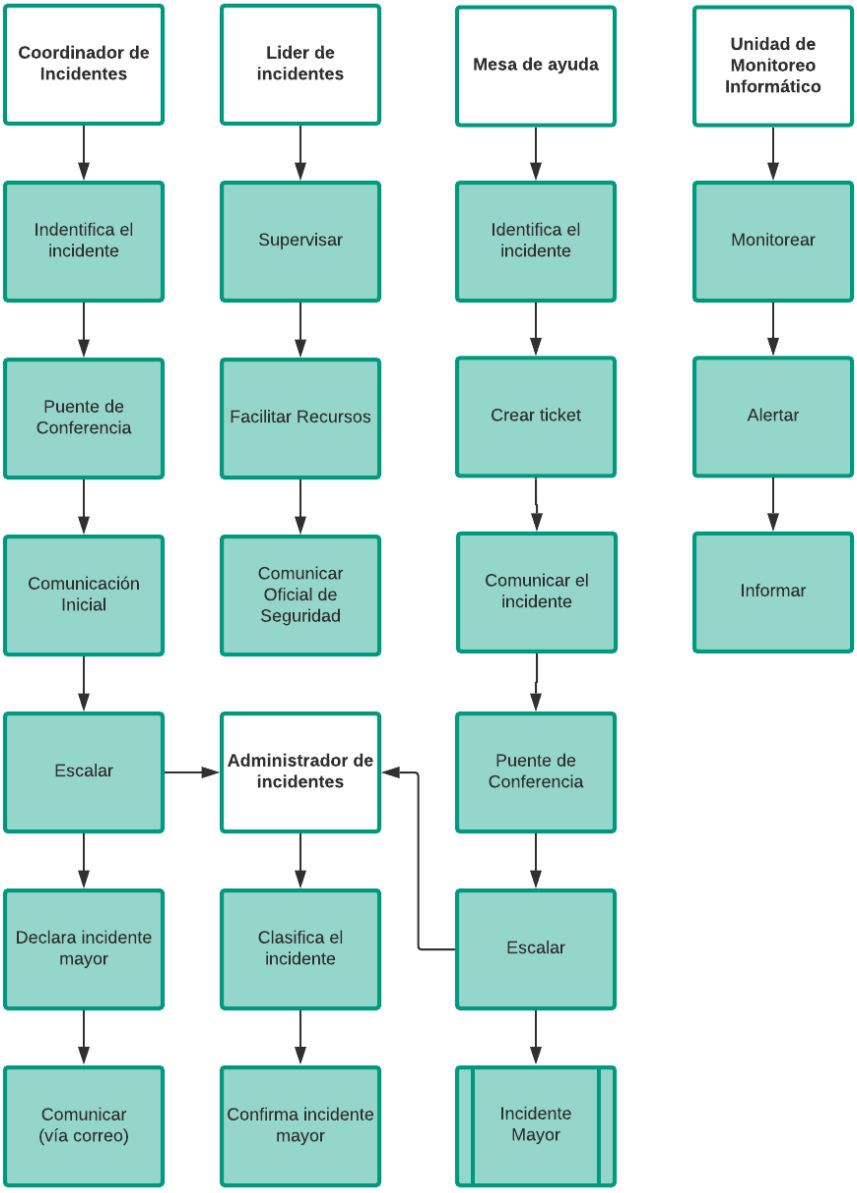


Fig. 4 Propuesta de los procesos según estructura organizacional de Gestión de Incidentes.

2.2.1 Coordinador de Incidentes y sus responsabilidades

El coordinador de incidentes es un punto de contacto único para iniciar la respuesta a incidentes mayores. Siempre está disponible las 24 horas, los 7 días de la semana, trabaja en estrecha relación con el administrador de incidentes para facilitar la respuesta y la resolución durante todo el ciclo de vida de todos los incidentes mayores (ver anexo 2, 3, 4, 5 y 8).

Simplemente Facilita el proceso de incidentes mayores a través de la coordinación, documentación y comunicación.

El coordinador de incidentes es responsable de lo siguiente:

- Realizar informes iniciales (indagarse de los primeros indicios).
- Confirmar la declaración de incidente mayor.
- Iniciar, facilitar y participar el puente de conferencia.
- Coordinar los recursos necesarios para solucionar problemas, comunicarse y / o tomar decisiones para resolver un incidente mayor.
- Asegurar los procedimientos en los procesos y las actualizaciones, la comunicación, la documentación y la escalada
- Registrar los incidentes importantes y detallar la resolución a través de http://servicios.dis.dgi.gob.ni
- Crear un registro de problemas para cada incidente mayor.
- Abrir un ticket de incidente mayor y mantener un registro continuo de eventos.
- Mantener los tiempos de actualización de escalado y comunicaciones asociadas con recursos técnicos, propietarios de servicios y administración.
- Asegurar que las comunicaciones internas de incidente mayor se realicen de manera oportuna, incluyendo:
    - Alertas DIS al principio y en su resolución.
    - Publicaciones en el sitio web de DIS (www.dis.dgi.gob.ni)
- Crear un registro de problemas relacionados.
- Investigar e implementar nuevas herramientas de control.

2.2.2 Administrador de Incidentes y sus responsabilidades

Un administrador de incidentes es el responsable de la restauración de un servicio interrumpido o degradado.

El administrador de incidentes es responsable de lo siguiente:

- Confirmar y clasificar Incidentes mayores, en función del impacto institucional.
- Liderar el esfuerzo de resolución de problemas:
    - Identificar, reunir y desplegar recursos técnicos.
    - Dirigir la discusión sobre el puente de la conferencia primaria (y coordinar con el puente técnico, si corresponde).
- Aprobar la solución propuesta o la solución alternativa.
- Confirmar la resolución del incidente mayor.
- Comunicarse con las partes interesadas y los usuarios finales.

- Responsable de la revisión posterior a la acción:
    - Revisar y validar el registro de eventos.
    - Determinar e implementar medidas preventivas y próximos pasos.

2.2.3 Líder de incidentes y sus responsabilidades.

Tiene la responsabilidad de llevar el progreso hacia la restauración del servicio durante el incidente mayor de categoría 2 (si se extiende) o de categoría 3.

El líder de incidentes es responsable de lo siguiente:

- Supervisa la restauración del servicio a un alto nivel.
- Es responsable de comunicarse con el oficial de seguridad de la información y las principales partes interesadas de alto nivel.
- Facilita la disponibilidad de recursos de solución de problemas asociados por ejemplo, borrar calendarios, eliminar barreras).
- Supervisa las decisiones sobre las actividades de restauración que afectan a otros servicios no afectados.
- Tiene discreción para movilizar recursos a través de la DIS (por ejemplo, otras áreas de servicio).
- Garantiza al oficial de seguridad de la información a decidir si el incidente es una Crisis.

2.2.4 Mesa de ayuda (GASI).

La primera persona contactada por un usuario final (independientemente del título) es la primera línea. Se espera que esta persona abra el ticket, recopile y analice la información relevante del usuario y lo guíe a través del proceso de regresar a la operación normal o escale el ticket de Incidente al grupo apropiado (ver anexo 6).

Estos recursos de primera línea, incluso fuera de horario, podrían ser los primeros en identificar un incidente mayor.

2.2.5 Responsabilidades Unidad de monitoreo informático (UMOI).

- Asegurar que se asignen recursos adecuados en los presupuestos de la DIS para cubrir las actividades, incluyendo revisiones de monitoreo, evaluaciones externas y RDA.
- Asegurar que la unidad de monitoreo funcione de manera satisfactoria.

- Revisar periódicamente los sistemas para que se adapten adecuadamente a los contextos operativos cambiantes de la DIS.
- Asegurar que se brinde información (informes) relevantes y oportunos en formatos fáciles de usar a las partes interesadas principales, la Dirección superior de informática y usuarios.
- Proporcionar capacitación para el personal.

Responsabilidades adicionales para los involucrados en la respuesta a incidentes de seguridad de la información.

Se detallarán las responsabilidades del equipo o cualquier recurso técnico de la División de informática y sistemas (Infraestructura, Desarrollo, Operaciones, etc.) que reciba alertas o escaladas o que tenga un rol en la restauración de las operaciones normales (ver anexo 10).

- Identificar y escalar un incidente mayor al coordinador de incidentes.
- Participar en el puente de la conferencia, si corresponde.
    - Unirse al puente de conferencia dentro de los 15 minutos de la alerta DIS o el contacto de guardia.
    - Si no está disponible, una alternativa debe ser previamente identificada y fácilmente accesible.
- Comprender el panorama técnico, que incluye:
    - Dependencias técnicas o de servicio, como los efectos secundarios.
    - Cambios recientes que se realizan.
- Solucionar y trabajar para resolver incidentes de acuerdo con los procedimientos establecidos.
- Ayudar a documentar los detalles del incidente y cualquier paso tomado para resolver el problema.
- Proporcionar actualizaciones periódicas al Administrador de incidentes y / o al Coordinador de incidentes sobre el estado de la investigación y la resolución del incidente.

2.2 Principales Incidentes de seguridad de la información reportados dentro de la DIS.

Tipo de incidente	Etapas	Nivel de prioridad	Acción recomendada
Escaneo de puertos	Reconocimiento	Normal	Ignore la mayoría de estos eventos al menos que la IP de origen tenga una mala reputación conocida, y haya múltiples eventos de esta misma IP en un período de tiempo pequeño.
Infección malware	Entrega y ataque	Alta-Incidente mayor	Corrija cualquier infección de malware lo antes posible antes de que avance. Escanee el resto de su red en busca de indicadores.
Denegación de servicio distribuida	Explotación e instalación	Critico	Configure servidores web para proteger contra las solicitudes de inundación HTTP y SYN. Configure su IPS durante un ataque para bloquear las IP de origen. A veces se usa un DDoS para desviar la atención de otro intento de ataque más serio. Aumente el monitoreo e investigue todas las actividades relacionadas, y trabaje en estrecha colaboración con su proveedor de servicios.
Acceso no autorizado	Explotación e instalación	Incidente Mayor	Detecta, supervisa e investiga intentos de acceso no autorizados, con prioridad en aquellos que son críticos para la misión y / o que contienen datos confidenciales.
Violación interna	Compromiso del sistema	Critico	Identifique las cuentas de usuario privilegiadas para todos los dominios, servidores, aplicaciones y dispositivos críticos. Asegúrese de que el monitoreo esté habilitado para todos los sistemas y para todos los eventos del sistema, y también asegúrese de que esté alimentando su infraestructura de monitoreo de registros.
Escalada de privilegio no autorizada	Explotación e instalación	Critico	Configure sus sistemas críticos para registrar todos los eventos de escalada privilegiada y configure alarmas para intentos de escalada de privilegios no autorizados.
Ataque destructivo	Compromiso del sistema	Critico	Copia de seguridad de todos los datos y sistemas críticos. Probar, documentar y actualizar los procedimientos de recuperación del sistema. Durante un compromiso del

			sistema: capture pruebas y documente todos los pasos de recuperación, así como todos los datos probatorios recopilados.
Amenaza persistente avanzada o ataque en varias etapas	Todas las etapas	Critico	Cualquiera de los eventos singulares que se enumeran aquí podría ser parte del peor tipo de incidente de seguridad imaginable el temido APT. Lo importante es ver cada evento a través de un contexto más amplio, uno que incorpore la última inteligencia de amenazas.
Falsas alarmas	Todas la etapas	Normal	Gran parte del trabajo de respuesta del incidente se gasta eliminando información irrelevante y eliminando falsos positivos. Estará constantemente ajustando la radio de monitoreo de seguridad para obtener la señal correcta.
Otros	Todas las etapas	Critico	La respuesta a incidentes es una disciplina de mejora continua. A medida que vea que más y más eventos se convierten en incidentes, descubrirá nuevas formas de clasificar esos incidentes, así como nuevas formas de evitar que ocurran en primer lugar.

2.2.1 Incidentes y Riesgos que pudieran ocasionar los incidentes de seguridad detectados en la División de informática y sistemas.

Aunque la DIS nunca puede estar segura de qué camino tomará un atacante a través de su red, los piratas informáticos suelen emplear una determinada metodología, es decir, una secuencia de etapas para infiltrarse en una red y robar datos. Cada etapa indica un cierto objetivo a lo largo del camino del atacante. Las últimas herramientas y técnicas de ataque son cada vez más sigilosas y, a menudo, se pueden ocultar a simple vista.

Incidentes	**Riesgo**
Escaneo de puertos	Detección de puertos abiertos primer paso para un ataque.
Infección por malware	Daños en computadoras, redes, o la pérdida de datos críticos de la institución.
Denegación de servicio distribuida	Saturación de los servidores
Acceso no autorizado y Violación interna	Robo, destrucción, pérdida o alteración accidental o ilícita de datos.
Escalada de privilegio no autorizada	Ganar más privilegios para acceder a la información.
Ataque destructivo	Daño de la información de los contribuyentes.
Amenaza persistente avanzada o ataque en varias etapas	Control de componentes y aplicaciones web.
Falsas alarmas	Utilización de recursos no necesarios.
Otros	Sin solución en el manejo de incidente.

Capítulo 3. Propuesta del manual de procedimientos de Gestión de incidentes de seguridad.

Los procedimientos ayudaran a quien lo utilice a establecer y desarrollar una gestión de información eficaz para detección, evaluación, reporte, decisión, confirmación, respuesta y equipo de respuesta, en toda la División de informática y Sistemas de la Dirección General de Ingresos.

3.1 Procesos y pasos de alto nivel de un incidente mayor

Se definieron los procedimientos de alto nivel, que van desde evaluar, contener, y resolver los incidentes.

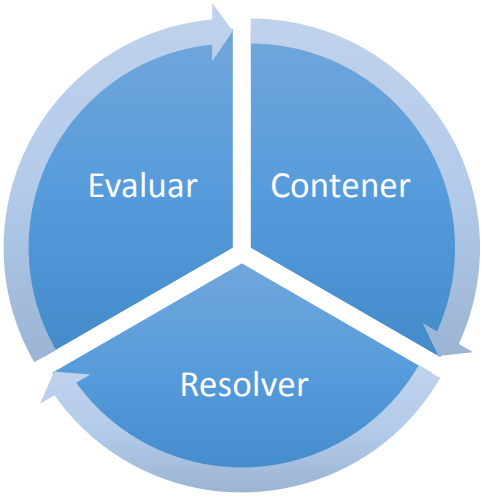


Fig. 5 Gráfica de manejo del incidente mayor

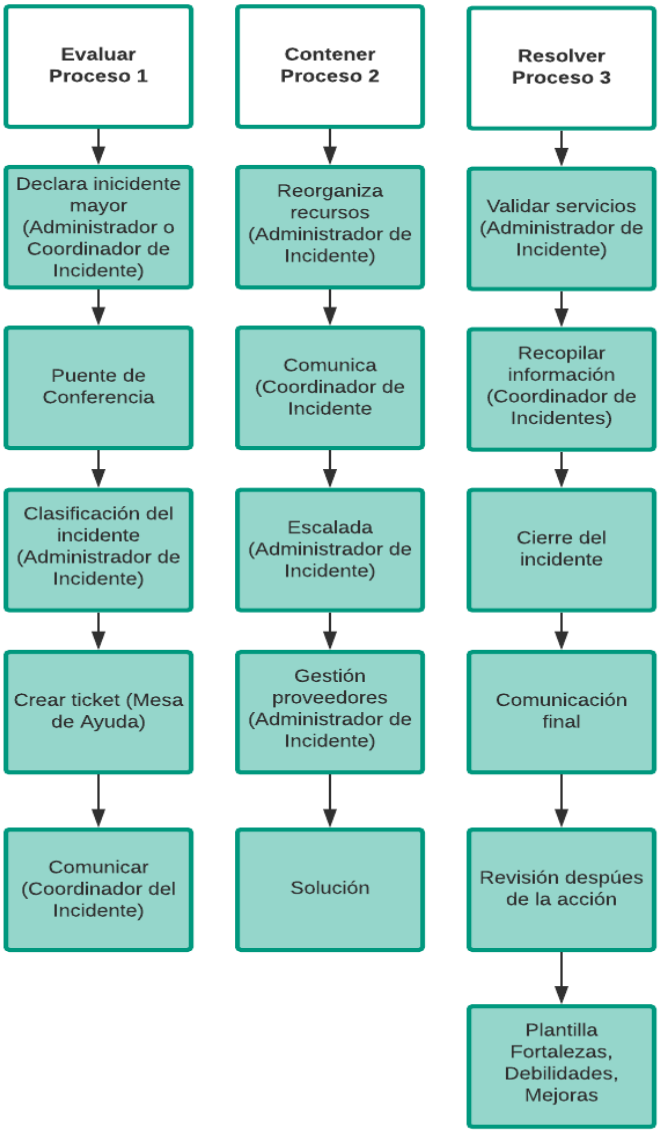


Fig. 6 Gráfica de los Procesos de un Incidente mayor.

3.1.1 Evaluar

Declaración del incidente mayor (ver anexo 1 flujo de trabajo de incidentes)

- Activado por informes de mesa de ayuda (GASI), monitoreo de eventos (UMOI) y / o personas.
- Recopilación de información preliminar sobre incidentes (Coordinador de incidentes).

Disparadores

Usuarios finales	Aumentos de tickets.
Personal (Staff)	Medidas preventivas, alertas, notificaciones internas y externas.

Criterios

Urgencia Intolerancia por retraso.	B	M	A
Riesgo de escalada Problema más generalizado.	B	M	A
Tamaño de la población.	B	M	A

Declarar incidente mayor, si dos criterios son M / A

Bajo: interrupciones menores del sistema que probablemente no serán visibles para ciertos usuarios o no afectarán las operaciones.

Medio: incidente que resulta en la pérdida o el compromiso de los datos de los usuarios, pero puede no desencadenar obligaciones formales de notificación. El problema comienza a propagarse.

Alto: incidente que desencadena obligaciones de informar, afecta a una gran cantidad de usuarios, y / o es destructivo para las operaciones de la institución.

Responsable de la declaración

- Administrador de incidentes
- Si el anterior no está disponible, Coordinador de incidentes.

Coordinación Inicial

Puente de conferencia: software o hardware dedicado, o línea telefónica separada, que la una institución utiliza para una discusión entre varias personas.

El coordinador de incidentes convoca al Administrador de Incidentes y al equipo técnico en el puente de la conferencia. (El puente de conferencia es crítico para solución eficiente de problemas y comunicaciones centralizadas).

- Todos las partes deben unirse en 15 minutos.
- Una vez que el Administrador de incidentes se une, dirige la llamada.
- Discusión inicial sobre el puente de conferencia:
    - Problema expresado.
    - Evaluar el impacto comercial.
    - Revise los cambios recientes.
    - Abra un puente técnico separado, si es necesario.

Nota: La actividad en el puente de conferencia debe centrarse principalmente en la restauración del servicio. La causa raíz es importante, pero generalmente debe seguir siendo secundaria. Siempre que sea posible, conserve la información forense para respaldar un análisis posterior y una revisión posterior a la acción.

Números de teléfono y acceso al puente de conferencia

Puente	**Líder**	**Participante**
Puente incidente mayor	3447#	3303#
Puente Secundario	3448#	3304#

Características del puente de conferencia

Líder	Alguien
***2** Inicia / Finaliza grabación	*0 Operador
***7** Bloquea / Desbloquea Conferencia	*6 Silencia y deja de silenciar tu línea
72# Lista de nombres	
80# Silencia todas las líneas	
81# Deja de silenciar todas las líneas	

Clasificación de Incidentes mayores

- El Administrador de incidentes proporciona una clasificación inicial.
    - Según el impacto real e informado por el usuario, el monitoreo de eventos, la disponibilidad de soluciones conocidas y potencial para convertirse en una crisis.
    - Si no se puede contactar al Administrador de incidentes, esta evaluación la determina el Coordinador del incidente.

- Se debe realizar una evaluación preliminar y luego actualizar cada 30 minutos (puede ser más tiempo, dependiendo de la investigación necesaria).
- Si no se identifica una posible solución en 2 horas, la categoría incidente mayor deberá ser actualizada.
- El administrador de incidentes puede ajustar la clasificación, además la información se recopila en función de las necesidades del negocio, etc.

Incidente de seguridad de la información

- Informar las operaciones de seguridad de la información de cualquier incidente.
- Los incidentes con un componente significativo de seguridad de la información deben tratarse de manera diferente al protocolo estándar de incidentes mayor.
    - Se debe asignar tiempo suficiente para una evaluación precisa y detallada del alcance del incidente.
    - Las comunicaciones externas e internas de la DIS a menudo son limitadas (por ejemplo, no hay ticket en GASI, no se registra en la DIS) para evitar "avisar" al autor (ya sea a través de nuestros canales públicos o propios) y minimizar el evento.
- Para estos incidentes, el oficial de seguridad de la información (o designado) actúa como Líder de Incidentes.

Comunicación inicial de un incidente mayor (ver anexo 7)

- El coordinador de incidentes crea un ticket en http://servicios.dis.dgi.gob.ni canal principal sobre el progreso para actualizaciones internas.
- Cadena de comunicaciones iniciada para la categoría 2 o categoría 3.
- Administrador de incidentes >Líder de incidentes > Oficial de Seguridad de la información.
- El coordinador de incidentes notifica al personal DIS.
    - Alertas DIS
    - Sitio web DIS
- Actualización del mensaje telefónico de la mesa de ayuda con pasos específicos de la información.
- El administrador de incidentes notifica a los usuarios y partes interesadas.

3.1.2 Contener

Investigación y diagnostico

- Reorganización de los recursos de solución de problemas apropiados (Administrador de incidentes)
- Comunicación continua (Administrador de incidentes)
- Escalamiento según sea necesario (Administrador de incidentes o Coordinador de incidentes)
- Gestión de proveedores según sea necesario (Administrador de incidentes)
- Implemente una solución temporal o una solución permanente (Administrador de incidentes).

Guía de Principios y procedimientos

- Busque múltiples guías potenciales y flujos de trabajo paralelos, según corresponda.
- Evite combinar incidentes aparentemente relacionados.
    - Continúe resolviendo problemas como incidentes separados hasta que se confirme que están relacionados.
- Revise cambios de calendario para identificar cualquier posible causa o impacto.
- Siga las listas de verificación de solución de problemas; Aproveche los flujos de trabajo o los mapas de servicio (si están disponibles).

Coordinador de incidentes

- Documentación de todo el material técnico, procesos, comunicaciones e información relacionada con el ticket.
- Alertas DIS adicionales, si la categoría de incidente mayor cambia.

Administrador de incidentes

- Investigación técnica y diagnóstico.
- Reorganización de los recursos de solución de problemas.
- Lanzar el puente de la segunda conferencia para discusiones técnicas, si necesario; coordinar entre dos conferencias para asegurar actualizaciones.
- Gestión de proveedores según sea necesario.
- Actualizaciones de estado en curso para las necesidades de comunicación.

Líder de incidentes

• Actualizaciones por hora al Oficial de Seguridad y a nivel superior también las partes interesadas.

Técnica de Escalada

- Las escaladas aumentan la participación y la conciencia del incidente a conjuntos de habilidades más avanzadas o niveles superiores de toma de decisiones.
- El Administrador de incidentes es responsable del proceso general de escalamiento.
- El nivel actual notifica al siguiente nivel a más tardar la hora siguiente hora indicada.

NMTQ* Horas	**Técnicos**
Comienza la solución de problemas	Jefes de área, desarrolladores, etc.
2	Oficial de Seguridad de la información
4	Proveedores (si es necesario)

*No más tarde que

3.1.3. Resolver

Resolución y cierre

- Validación de que todos los servicios están operativos, incluido el posterior (Administrador de incidentes).
- Recopilación de toda la información clave, por ejemplo, hora de finalización, acciones, causa raíz cuando se conoce (Administrador de incidentes y Coordinador de Incidentes).
- Comunicación final, incluida la notificación de resolución de alerta DIS (Coordinador de incidentes).
- Revisión del problema de activación y revisión posterior a la acción.

Resolución

- El Administrador de incidentes valida que todos los servicios estén operativos, incluyendo aquellos que no están en línea.
- El coordinador de incidentes reúne toda la información clave por ejemplo, hora de finalización, acciones, causa raíz (cuando se conoce) y se incluye en el ticket.

Cierre de incidentes

- Comunicación final, incluida la notificación de resolución de alerta DIS.
- Revisión del problema y revisión posterior a la acción para todos los involucrados.
    - Reuniones de gestión de problemas
    - Confirmar / actualizar causa raíz.
    - Abordar cualquier problema o inquietud abierta.
    - Identificar la mitigación necesaria y los próximos pasos, se incluyen los propios y programados.

Revisión después de la acción

El aprendizaje de la División de informática y sistemas requiere que los equipos evalúen continuamente su desempeño para identificar y aprender de los éxitos y fracasos. A continuación se define plantilla para identificar fortalezas, debilidades y mejoras en la gestión de incidentes.

Plantilla Fortalezas, Debilidades y Mejoras

• **# Incidente**_____

• **Duración**_____

- Fecha de inicio_____Fecha final_____Tiempo Total_____

• **Sistemas afectados**_____

_____

• **Indicios**_____

_____

• **Cronología y Resumen de eventos**_____

_____

_____

_____

• **Solución Alternativa / Solución Final**_____

_____

_____

_____

• **Análisis de raíz de la causa**_____

_____

-Técnica_____

_____

_____

• **Proceso y Revisión de comunicación**

- ¿Qué salió bien?_____

- ¿Qué se puede mejorar?_____

_____

_____

• **Próximos pasos**

- Medidas preventivas para prevenir la recurrencia_____

_____

_____

- Recomendaciones_____

_____

_____

3.2 Código de conducta

Se definió la forma de actuar de los involucrados ante las actividades de gestión de incidentes de seguridad de la información de la División de informática y sistemas.

Generales

- **Recuerde actuar de acuerdo con los valores DIS** (es decir, usuario centrado, colaborativo, innovador y abierto), especialmente durante los períodos críticos.
    - Centrado: asuma la responsabilidad personal de resolver la situación. Defienda cualquier compromiso que haga.
    - Colaborativo: descubra quién puede ayudar al comunicarse con otros equipos y esté listo para ofrecer su conocimiento y experiencia.
    - Innovador: obtenga buena información para recomendar soluciones apropiadas.
    - Abierto: trate a todos con respeto; escuche y responda con empatía.
- **Informar los problemas**: llame a la línea directa ext. 3323.
    - Evite las llamadas innecesarias a la mesa de ayuda (GASI) o al personal.
    - **En caso de crisis**, las llamadas pueden hacerse directamente al líder de incidentes.
- **Responda rápidamente** cuando el coordinador de incidentes se comunique con usted.
    - Llame al puente de conferencia lo antes posible, a más tardar en 15 minutos después de la notificación.
- **Respete los procesos** para garantizar una resolución eficiente y una buena colaboración.
- Limite el puente de conferencia al personal principal: evite los participantes innecesarios, esto dificulta el progreso y la comunicación clara.
- **Asegure el acceso oportuno al personal apropiado** (usted mismo u otros).
    - Mantenga y comparta listas de información actualizadas sobre llamadas, personal (incluidas las que están de vacaciones y los de apoyo) y números de teléfono.
    - Proporcionar acceso fácilmente disponible a la experiencia técnica necesaria (especialmente en tiempos de escalada o transición).
    - Dedique su tiempo o el de su equipo según lo justificado y la atención para garantizar la restauración rápida del servicio.

- **Coordinar las comunicaciones internas:** el material para la resolución de problemas, las comunicaciones y las decisiones deben comunicarse / validarse en el puente de conferencia y en el ticket.

En caso de solicitudes externas

¿Qué debe hacer si las autoridades nacionales solicitan información?

- De vez en cuando, la institución Policía Nacional u otro organismo jurídico o de seguridad nacional, puede formalmente (con una solicitud por escrito o una citación) o de manera informal (sin documentación escrita) pedirnos que proporcione información sobre las actividades de personas que usan redes o sistemas de la División de informática y sistemas de la Dirección General de ingresos de Nicaragua o para solicitar datos específicos, como copias de archivos o correo electrónico.
- Si recibe tales solicitudes, informe al solicitante que no tiene la autoridad para responder tales solicitudes por su cuenta. Según las reglas de la División de informática y sistemas, el personal debe contactar a la Oficina del Asuntos Legales y Asesoría legal. La Oficina de Asuntos Legales y asesoría legal de la DGI debe evaluar las solicitudes y determinar cómo responder.
- Si tiene buenas razones para pensar que existe una amenaza para la salud o la seguridad de la información en general proporcione información reducida, luego debe proporcionar toda la información en dependencia lo solicitado.

Mesa de ayuda (GASI).

- **Enfoque del usuario**: reconozca la importancia del problema del usuario. Trate al usuario final como le gustaría que lo tratara una organización de servicios. Transmita empatía por la situación con su tono y palabras: "Entiendo, podemos ayudarlo con eso, lamento que esto haya sucedido..." Mantenga toda la comunicación cortés, clara (no técnica), apropiada hasta el punto de solo compartir información que sea aplicable para resolver su problema.
- **Colaboración:** trate a los equipos de la DIS como desee que lo traten. Pida ayuda a sus colegas en tiempo real cuando sea posible para obtener una resolución más rápida. Ayude a los equipos de la DIS con resoluciones técnicas y mejoras de procesos. Ponga al usuario y la resolución primero, es decir, obtenga la información necesaria, arregle el proceso después de la resolución.

- **Sea proactivo:** "Me alegra que hayamos podido resolver su problema actual, ¿hay algo más en lo que pueda ayudarlo?"
- **Comuníquese con los equipos de la DIS con urgencia:** llame a los Jefes de área, cuando no esté seguro de dónde debe ir el ticket a continuación y o si cree que el ticket asignado se perdió.

3.3 Procedimientos para incidentes mayores.

El objetivo del proceso de incidente mayor es resolver los Incidentes lo más rápido posible, se espera que todos los miembros del personal del equipo de respuesta a incidentes (IRT) registren el Incidente mayor. Se proporcionará tanta información como sea posible para facilitar el proceso.

- Minimizar el impacto negativo para la institución y su misión.
- Restaurar el servicio normal lo más rápido posible.
    - Implementar una solución alternativa, si permite una resolución más rápida.
    - Equilibrar la restauración del servicio (gestión de incidentes) con la recopilación de información de causa raíz (gestión de problemas).
- Oficial de seguridad necesita el personal y los recursos necesarios para la resolución.
- Comunicar de manera apropiada y oportuna.
    - Interno: DIS, incluido los lideres según sea necesario.
    - Externo: usuarios y partes interesadas.

Reportar Incidentes Mayores

Un incidente mayor es un incidente que provoca una interrupción significativa del negocio y exige una respuesta más allá del proceso de administración de incidentes de rutina. Los incidentes mayores tienen un procedimiento separado con plazos y urgencias más cortos que se requieren para acelerar el proceso de resolución de incidentes con alto impacto en el negocio.

Será el equipo técnico de la División de informática y sistemas quien decidirá si se deben reportar y registrar dichos casos a través de los mecanismos. De lo contrario, se debería dejar en claro al personal cuál es el proceso alternativo para incidentes.

- Si cree que puede haber un incidente mayor, llame a la línea directa.

Llame a la línea directa en cualquier momento Ext. 3323

- Proporcione tanta información como sea posible para facilitar el proceso:
    - Hora de inicio del incidente
    - Servicios o aplicaciones afectados
    - Impacto en los usuarios o las funciones de la División de informática y sistemas.
    - Los equipos necesitan solución de problemas.
    - Diagnóstico inicial o acciones actuales, si las hay.

3.3.1 Procedimientos iniciales de incidentes mayores.

Identificación de incidentes mayores

Los incidentes mayores generalmente se identifican de una de dos maneras:

1) Usuarios de un servicio o un equipo técnico llama a la Línea Directa de la mesa de ayuda (**GASI**) con un evento confirmado que impacta el servicio. En esta situación, el Coordinador de incidentes y el Administrador de incidentes usan en colaboración la matriz de Criterios de incidente mayor para confirmar si debe ser declarado o no. La decisión final es responsabilidad del Administrador de incidentes. Sin embargo, el Coordinador de incidentes asume esta responsabilidad si el Administrador de incidentes no está disponible.

2) Cualquier miembro del personal de la DIS puede notificar al Coordinador de Incidentes de un presunto incidente mayor. El ejemplo más probable es un aumento de tickets similares en la mesa de ayuda. En esta situación, el Coordinador de incidentes debe confirmar que se ha producido una solución adecuada de problemas, duplicación de indicios y recopilación de detalles. Póngase en contacto con Recursos técnicos para obtener confirmación adicional según sea necesario. Una vez que se ha reunido suficiente información, el Coordinador de incidentes debe comunicarse con el Propietario del servicio y utilizar en colaboración la matriz de Criterios de incidente mayor para confirmar si debe ser declarado o no.

Coordinación de recursos

Una vez que el administrador de incidentes ha confirmado o declarado un Incidente mayor, el Coordinador de incidentes es responsable de contactar y coordinar los recursos técnicos necesarios para diagnosticar y resolver el incidente. Para garantizar una respuesta rápida, las escaladas de recursos técnicos se manejan mediante llamadas telefónicas al número de guardia de cada grupo. Deje un mensaje si el personal de guardia no contesta el teléfono. Su llamada debe ser devuelta dentro de los 15 minutos. De lo contrario, el Coordinador de incidentes debe escalar al director del grupo.

NOTA: La lista actual de teléfonos de llamadas y escalada se mantiene en GASI http://servicios.dis.dgi.gob.ni y está disponible https://directorio.dgi.gob.ni

Durante las escaladas, el Coordinador de incidentes debe:

- Transmitir los detalles y la urgencia de la situación.
- Establecer el método y el cronograma para recibir actualizaciones del equipo técnico.
- Establecer un puente de conferencia, si es necesario.
- Comenzar la documentación del incidente mayor a través de tickets GASI.

Documentación inicial

Documentar un ticket de incidente mayor en la mesa de ayuda (GASI) implica dos pasos:

- Crear un ticket de incidente mayor.
- Completar los datos de incidente mayor.

1. Abra http://servicios.dis.dgi.gob.ni y cree un nuevo ticket.

2. Ingrese la información requerida.

Usuario	Original Coordinador de incidentes
Servicio	El servicio o aplicación DIS más afectado por ejemplo: mail.dgi.gob.ni
Categoría	La categoría debe ser la resolución de problemas o la interrupción del servicio, si está disponible.
Grupo de asignación	Grupo primario del coordinador de incidentes actual.
Asignado a	Esto siempre debe ser el Coordinador de incidentes actual
Descripción breve	debe ser "<nombre del servicio> Interrupción o degradación"
Descripción	Descripción del informe inicial de incidentes mayores, quién informó, a qué hora, detalles, etc.

3. Establezca el Impacto y la Urgencia para que la Prioridad se convierta en "1 - Incidente mayor"

Estado Incidente mayor	Establezca esto en "Alertas" para un nuevo incidente mayor
Categoría incidente mayor	Un incidente mayor generalmente comenzará en la Categoría 1, pero se puede escalar a solicitud del Administrador de incidentes si el alcance del incidente es significativo.

Servicios afectados	Los servicios DIS o las aplicaciones afectadas por el incidente mayor.
Grupos involucrados	Equipos técnicos involucrados en la investigación y resolución de un incidente mayor
Grupo de propietarios	Equipo técnico que posee el servicio interrumpido y es responsable de la resolución de MI
Proveedor externo	Marque esta casilla para servicios alojados
Usuarios impactados	Use esto solo si el incidente mayor es específico de la población
Lugares afectados	Use esto solo si el incidente mayor es específico de la ubicación
Impacto al negocio	Descripción detallada del impacto para socios conocidos y procesos comerciales
Acciones actuales	Las acciones tomadas por los recursos técnicos para investigar o resolver el incidente.
Código de puente en Nueva actualización	El código de puente se completará automáticamente y se mostrará en cualquier alerta nueva o de actualización enviada
Incluir información del puente	Esta casilla debe estar marcada si se usará un puente de conferencia durante la respuesta Incidente mayor,
Tiempo reportado	Fecha y hora en que se informó al coordinador el incidente mayor.
Tiempo de interrupción del servicio	Fecha y hora confirmadas del estado del incidente mayor.
Servicio de tiempo de restauración	Fecha y hora de finalización confirmadas del incidente mayor, (se completará con la resolución).
Duración del incidente mayor	Duración de un incidente mayor en horas y minutos. Este campo se calculará automáticamente en la resolución.

Comunicaciones iniciales

Después de la creación inicial del ticket en la mesa de ayuda (**GASI**) como Coordinador de Incidentes, es responsable de comunicar de inmediato un incidente mayor.

Las comunicaciones pueden ser tanto internas como externas:

- Para todos los incidentes mayores, use el correo electrónico gasi@dgi.gob.ni para comunicarse con el personal DIS a través de Alertas DIS. Estos correos electrónicos requieren un nivel significativo de detalles técnicos. Realice un seguimiento de todas las actividades de comunicación.
- Para un incidente mayor externo, uno que afecte a servicios u organizaciones externos, use el correo gasi@dgi.gob.ni para comunicarse con los usuarios

finales. Estas correos deben contener muchos menos detalles técnicos que los requeridos por la notificación interna.

Si un incidente mayor no tiene ningún impacto para el usuario, no es necesario publicarlos y enviar correos electrónicos externos.

Comunicación inicial por correo electrónico interno: TODOS LOS INCIDENTES MAYORES

Utilice el correo gasi@dgi.gob.ni para comunicar todos los incidentes importantes al personal DIS sin importar el impacto.

Comunicación interna inicial - PUENTE DE CONFERENCIA

Un puente de conferencia permite a los operadores internos de su sistema telefónico y a las personas externas que llaman a su sistema telefónico la capacidad de colaborar e interactuar entre sí en una sola llamada telefónica. Se puede establecer reglas (como un código PIN) para obtener acceso a la llamada.

Distribuya el código del participante utilizando una alerta DIS.

Llame a la ext. 3323 e ingrese uno de los códigos líderes que se enumeran a continuación:

Puente primario:

- Código Líder: 71284835 #
- Participante: 38793366 #

Puente Secundario

- Código de líder 58775889 #
- Código de participante: 86065154 #

La agenda debe incluir como mínimo:

- Confirmar que el personal correcto está involucrado y escalar a personal adicional según sea necesario.
- Informar a todos los participantes sobre el impacto, los indicios y las acciones actuales en curso para resolver el incidente.
- Discutir el cronograma de actualización con los asistentes del puente de conferencia.

Plantilla Comunicación inicial nuevo incidente- SOLO IMPACTO EXTERNO

1. **Nombre del incidente:** debe coincidir con la breve descripción del ticket GASI de incidente.
2. **Estado del incidente:** seleccione la opción adecuada.
3. **Investigación:** aún no se ha identificado el alcance completo del Incidente mayor.
4. **Identificado:** se ha identificado el alcance del incidente mayor y se están realizando esfuerzos de resolución.
5. **Monitoreo:** el servicio ha sido restaurado pero el personal de la DIS, el grupo Unidad de monitoreo (UMOI) está monitoreando activamente el desempeño.
6. **Resuelto:** el servicio ha sido restaurado a operación normal.
7. **Mensaje:** un breve resumen del impacto del incidente.
8. Alertar a los usuarios suscritos de todos los servicios y aplicaciones afectados por el incidente mayor.
9. **Estados del Servicios:** estado apropiado para cada uno de los servicios afectados.
10. Se comunica el incidente.

3.3.2 Procedimientos de actualización de incidentes mayores.

Durante un Incidente mayor, el Administrador de Incidentes es responsable de liderar los esfuerzos de resolución.

Las responsabilidades del coordinador de incidentes incluyen:

- Asistir al administrador de incidentes con la coordinación de recursos
- Proporcionar orientación sobre el proceso.
- Asegurar de que se identifiquen los acontecimientos, las actualizaciones y los puntos de escalada.
- Documente la actividad en el ticket GASI.
- Enviar comunicaciones según sea necesario.

Actualizar un ticket de incidente mayor

Actualice un ticket de incidente mayor con la frecuencia necesaria para reflejar los cambios en el progreso de un incidente mayor. La información que debe tenerse en cuenta incluye:

- Puente de conferencia participantes.
- Pasos a tomar para la solución de problemas.

- Decisiones tomadas.
- Resumen de discusión.
- Siguiente acontecimiento o actualización programada.
- Escalamientos de categoría de incidente mayor.

Actualizaciones del incidente mayor y escalamientos de categoría

El Coordinador de incidentes debe colaborar con el Administrador de incidentes para establecer un cronograma para las actualizaciones del estado del incidente mayor, idealmente cada 30 minutos.

La mayoría de los incidentes importantes comienzan en la Categoría 1, pero el Administrador de incidentes puede clasificarlo con una Categoría diferente, según el impacto del usuario, la disponibilidad de soluciones conocidas o el potencial de convertirse en una crisis. La categoría inicial debe revisarse durante cada actualización de estado del incidente. Si no se identifica una solución posible dentro de las 2 horas, la categoría de incidente mayor debe escalarse.

En la Categoría 2, el Administrador de incidentes es responsable de garantizar que el Líder de incidentes participe según sea necesario.

En la Categoría 3, el Líder del incidente debe asumir la responsabilidad de los esfuerzos de resolución.

Es responsabilidad del coordinador de incidentes garantizar que se cumplan estas pautas de proceso.

Actualización de comunicaciones

Comunicación de actualización interna por correo electrónico: TODOS LOS INCIDENTES.

Envíe una actualización interna por correo electrónico gasi@dgi.gob.ni solo cuando se haya escalado la categoría de incidente mayor.

3.3.3 Procedimientos de resolución de incidentes mayores

El administrador de incidentes es responsable de declarar un incidente mayor que se resolverá después de la restauración del servicio. El coordinador de incidentes debe ayudar a coordinar los recursos para probar y confirmar la funcionalidad del servicio según sea necesario.

Después de la resolución del incidente mayor, el coordinador del incidente debe hacer lo siguiente:

- Actualizar y resolver el ticket GASI.
- Enviar notificación de resolución interna.

- Actualice la publicación del estado del servicio.
- Enviar notificación de resolución externa (si es necesario).

Actualice el ticket de incidente mayor para reflejar que el incidente principal se ha resuelto.

- Abra el Formulario de incidente mayor.
- Rellene los campos de resolución.

Nombre del campo	Notas de uso
Acciones de resolución	Acciones realizadas por el grupo técnico para resolver el incidente mayor
Análisis de raíz de la causa	Conocimiento actual del grupo técnico sobre la causa del incidente mayor, si está disponible
Causa principal	Si se identificó una causa raíz, informarla.
Próximos pasos	Puntos a seguir.
Seguimiento requerido	Después de la reunión de revisión de problemas

Comunicaciones de resolución

Resolución de correo electrónico interno - TODOS LOS INCIDENTES MAYORES.

Utilice el correo gasi@dgi.gob.ni para comunicar todos los incidentes importantes al personal DIS sin importar el impacto.

3.4 Procedimientos gestión de incidentes mesa de ayuda GASI

Primera línea (contacto inicial)

- Identificar y escalar un incidente mayor para el Coordinador de incidentes.
- Participar en el puente de la conferencia, si corresponde.
    - Unirse al puente de conferencia dentro de los 15 minutos de la alerta DIS o el contacto del grupo de monitoreo.
    - Si no está disponible, una alternativa debe ser previamente identificada y fácilmente accesible.
- Comprender el panorama técnico, que incluye:
    - Dependencias técnicas o de servicio, como los efectos posteriores.
    - Cambios recientes
- Solucionar problemas y trabajar para resolver incidentes de acuerdo con los procedimientos internos.
- Ayudar a documentar los detalles del incidente y cualquier material que se haya tomado para resolver el problema.
- Proporcionar actualizaciones periódicas al Administrador de incidentes y / o al Coordinador de incidentes sobre el estado de la investigación y la resolución del incidente.

Procedimientos de manejo de tickets

* Consulte el manual de procedimientos GASI, para saber cómo usar correctamente los estados del ticket (creados, en espera, prioridad del ticket, cerrados, etc.).

- Actualice los tickets diariamente, principalmente durante todo el día en tiempo real, en lugar de guardar todas las actualizaciones y resoluciones hasta el final del día.
    - En tiempos de mucho volumen de tickets, la frecuencia será cada dos días.
- Comuníquese directa y frecuentemente con los usuarios finales durante todo el ciclo de vida del ticket y, una vez resuelto, con información clara, precisa, (no técnica) y significativa para ellos.
- Verifique todos los tickets asignados antes del final de su turno, para buscar problemas URGENTES. Esto no significa que tenga que quedarse después de su turno para resolverlo, pero sí tiene que escalarlos a alguien que pueda; su supervisor o Jefe.

    - Cuando mueva tickets a otro grupo, incluya tanta información detallada como sea posible.Asegúrese de saber a dónde debe ir el ticket, pregúntele a un compañero si puede.
- Contacto con el usuario: si un usuario no responde a las consultas, comuníquese; ponga el ticket en espera e intente contactar por correo electrónico 2 veces y por teléfono 1 vez dentro de los 5 días hábiles. Tenga en cuenta todos los intentos de contacto del ticket.
    - Si no se alcanza al usuario final dentro de ese tiempo, resuelva con el motivo e instruya al usuario sobre cómo abrir un nuevo ticket.
- Aproveche a sus compañeros de equipo cuando tenga preguntas sobre un problema que no puede resolver y, si es necesario, diríjase a un líder de equipo, supervisor o Jefe.
- Si un ticket carece de información, comuníquese directamente con el usuario para obtener información y mantener el proceso en movimiento. NO lo envíe de vuelta a su lugar de origen para solicitar más información. Obtenga la información que necesita y trabaje hacia la resolución. Seguimiento de la falta de información después del hecho.
- Los ticket de incidente mayor se deben manejar / resolver o escalar de inmediato.
    - Estos tickets se deben mantener en movimiento.
- Todos los tickets de incidentes que esperan más información de un usuario / proveedor deben quedar en espera.
- Tenga en cuenta los MTTR (Mean Time to Recovery) tiempo medio de recuperación, en todos los tickets, no cierre un ticket apresuradamente, asegúrese de que sepa que su problema está solucionado, para evitar que un ticket sea reabierto.
- Si un usuario responde a un correo electrónico de ticket resuelto con un problema nuevo, cree un ticket nuevo para el problema nuevo e informe al usuario del procedimiento a seguir: envíe un correo electrónico a gasi@dgi.gob.ni

Procedimientos de manejo de incidentes durante ausencias, personal mesa de ayuda (GASI).

Ausencia planificada

- Antes de cualquier ausencia de un empleado por cualquier duración, el empleado resolverá o actualizará todo los tickets asignados según lo permita el tiempo.

- Los tickets de alta prioridad asignados al ausente que no se resuelvan, serán reasignados a otro técnico por los líderes GASI.
- Si la ausencia es por un día o menos, los casos asignados y en espera (no urgentes) permanecerán asignados al ausente y actualizados por los líderes del equipo el día de la ausencia según lo permita el tiempo.
- Si la duración de la ausencia es de dos o más días, los líderes GASI reasignarán todas las entradas asignadas al ausente.

Ausencia inesperada

- Ausencia estimada no más de un día.
- Los líderes GASI revisarán las entradas asignadas del ausente por la mañana o una vez que el supervisor haya enviado el aviso de ausencia.
- Los tickets de alta prioridad serán actualizados y / o resueltos inmediatamente por los líderes GASI o reasignados a otro técnico disponible.
- Los tickets en el estado asignado se reasignarán a otro técnico disponible para actualizar ese día.
- Los casos no urgentes y en espera permanecerán asignados al ausente y actualizados por los líderes GASI según lo permita el tiempo.
- Ausencias que duran más de un día.
- Los tickets restantes asignados al ausente serán reasignados por los líderes GASI una vez que el supervisor haya enviado el aviso de ausencia.

*Si va a estar fuera de la oficina, de vacaciones, se configurará un correo alternativo (personal) donde recibirá notificaciones sobre actualizaciones de sus tickets.

Todos los líderes GASI.

- Haga un seguimiento de los resultados estadísticos, (tiempos de respuesta, ticket resueltos por empleado etc.) para obtener más detalles sobre la experiencia.
- Revise activamente los tickets asignados al equipo GASI diariamente. Intervenga y / o mueva tickets a otros técnicos cuando sea necesario.
- Asegúrese de que los tickets no estén tardando en ser resueltos más de lo necesario.

3.5 Propuesta de Protocolos para incidentes de seguridad de la información DIS.

El personal de seguridad de la información de la División de informática de la Dirección General de Ingresos de Nicaragua se adhiere a la Política de acceso a la información electrónica. Estos protocolos explican cómo aplicamos la política a nuestras operaciones y guían al personal de seguridad de la información cuando deben tomar medidas inmediatas para proteger la seguridad general de la red y los sistemas. Se basan en los conceptos del Código de conducta profesional de la División de informática y sistemas (DIS) para proteger la información electrónica.

- Bloqueamos el acceso a los servidores y sitios de Internet solo cuando se utilizan para atacar los recursos de la DIS.
- Bloqueamos las cuentas de usuarios no privilegiadas sin previo aviso solo cuando hay evidencia clara de que una parte no autorizada las está utilizando.
- Eliminamos los sistemas de la red sin previo aviso solo cuando tenemos evidencia clara de que están comprometidos y que albergan o pueden proporcionar acceso a información confidencial de la DIS, o que se están utilizando para atacar otros sistemas.
- Bloqueamos la entrega de correos electrónicos solo cuando tenemos un alto grado de confianza de que el correo electrónico contiene software malicioso, dirige a los usuarios a instalar software malicioso o se está utilizando para recolectar contraseñas u otra información confidencial.
- Desactivamos los correos electrónicos de los servidores de correo electrónico de la DIS, solo cuando cumplen con los criterios anteriores y representan un riesgo crítico.
- Solo vemos los datos de registro agregados para cumplir con nuestra responsabilidad de proteger los datos y los sistemas.
- Vemos los datos de registro de las personas (siempre que sea posible, separados del nombre de una persona real) solo para cumplir con nuestra responsabilidad de proteger los datos y los sistemas, cuando el personal de la DIS lo autorice según lo definido en la Política de acceso a la información electrónica o, como se incluye en esa política, cuando la salud, la vida o la seguridad de una persona o personas pueden estar en riesgo.
- Notificamos a los usuarios lo antes posible cuando tomamos una acción que afecta su cuenta o sistema específico.
- Si tiene preguntas sobre las prácticas de seguridad que no se abordan en estos procedimientos, le recomendamos que se comunique con la oficina de seguridad de la información.
- Cuando sea posible, preservar el análisis forense para su posterior análisis.

3.6 Matriz RACI para roles clave durante incidentes mayores.

Se elaboró Matriz RACI para funciones claves durante incidentes mayores.

"La matriz RACI define ¿Quién es el responsable?, ¿Quién debe rendir cuentas?, y ¿a quién se debe consultar e informar dentro de un marco de trabajo orgánico?", (Oswaldo Fonseca Luna, 2013).

Actividad	**Líder de incidentes (categoría 2 y 3)**	**Coordinador de incidentes**	**Administrador de incidentes**	**Mesa de ayuda**	**Grupo de monitoreo (UMOI)**	**Recursos técnicos**	**Administrador línea técnica**
Identificación de incidentes	C	A	R	R	R	R	R
Coordinación inicial	C	A	C	C	C	C	C
Puente de conferencia + Ticket abierto	R	A	R	R	R	R	R
Comunicaciones iniciales	R	A	C	C	C	C	C
Solución de problemas	C/R	C/R	A	C/R	C/R	C/R	C/R
Investigación técnica y Diagnostico	R	C	A	C	C	R	R
Escalada	R	A	R	R	R	R	R
Comunicación continua	R	R	A	C	C	C	C
Documentación de incidentes	C	A	C	C/R	C/R	C/R	C/R
Resolución	C/R	C/R	A	C/R	C/R	C/R	C/R
Revisión después de la acción	R	R	A	R	R	R	R

*R: responsable *C: consultado *A: quien aprueba

VII. Conclusiones

Las responsabilidades en seguridad de la información no son fijas, se crean, eliminan y modifican con el tiempo, las regulaciones, las organizaciones, las tecnologías, etc. Es responsabilidad de la oficina de seguridad informática trabajar para garantizar el bienestar de los usuarios, la infraestructura y la tecnología DIS. La responsabilidad clave radica en proteger y garantizar que se mantenga la confidencialidad, la integridad y la disponibilidad, el resto puede colocarse en otras categorías.

Actualmente la forma de actuar de los usuarios DIS ante los incidentes de seguridad de la información es básica, solo cumplen la función de informar a los jefes de área los eventos y estos tomar la decisión de resolverlos. Por razones jerárquicas el mejor equipo de respuesta tiene que estar distribuido entre las diferentes áreas de los servicios afectados.

El presente trabajo permite ordenar y clasificar mejor los incidentes, involucra cambios en la DIS que implica cambiar la forma de trabajo de los usuarios para la atención de incidentes, definiendo procesos, roles, responsabilidades, formas de reporte y procesos a otro nivel. Si bien el proyecto muestra mejoras, tiene que ser aprobado y autorizado por el Director de la DGI.

Se identificaron incidentes a través del monitoreo temprano esto permitió disminuir la carga de trabajo del equipo de mesa de ayuda (GASI), ya que se pudieron detectar tempranamente alertas y eventos y cada propietario de servicio según sus procedimientos volver a la continuidad del negocio. Si bien la parte de gestión de incidentes no está implementada, estos procedimientos propuestos nos muestran que este manual es necesario.

Este documento servirá como el proceso oficial de gestión de incidentes para la División de informática y Sistemas de la Dirección General de Ingresos, para apoyar la oficina de seguridad informática nueva en el organigrama de la institución.

La División de informática y sistemas brindó algunas facilidades para obtener información confidencial de sus servicios e instalaciones, algunos datos fueron cambiados por acuerdos alcanzados de confidencialidad.

VIII. Recomendaciones

La División de informática y sistemas DIS, a menudo sufre de falta de recursos, tecnología o reconocimiento del tipo y magnitud del problema. Además, no tienen software, pruebas, procesos, tecnología o personas para manejar amenazas sofisticadas de seguridad de la información. Sin embargo, puede responder a incidentes de seguridad de la información de una manera más rápida y efectiva a través de los procedimientos propuestos. Esto se logra:

• Comprendiendo una serie de conceptos clave (por ejemplo, una definición de respuesta a incidentes de seguridad de la información; tipos de ataques; los principales desafíos y formas en que se pueden responder)

• Determinando el estado de preparación de los analistas de las diferentes áreas para responder a un incidente de seguridad de la información.

• Participando en iniciativas patrocinadas por el gobierno y otras relacionadas con incidentes de seguridad de la información o respuesta a incidentes.

• Adoptando un enfoque sistemático y estructurado para la gestión de incidentes de seguridad de la información, considerando las acciones clave que es posible que deba tomarlo cuando se evalué, contenga y resuelva un incidente.

• Seleccionando un proveedor o proveedores apropiados de experiencia en respuesta a incidentes de seguridad que puedan cumplir con más eficacia sus requisitos, pero al precio correcto, considerando un conjunto de criterios de selección acordados.

IX. Bibliografía

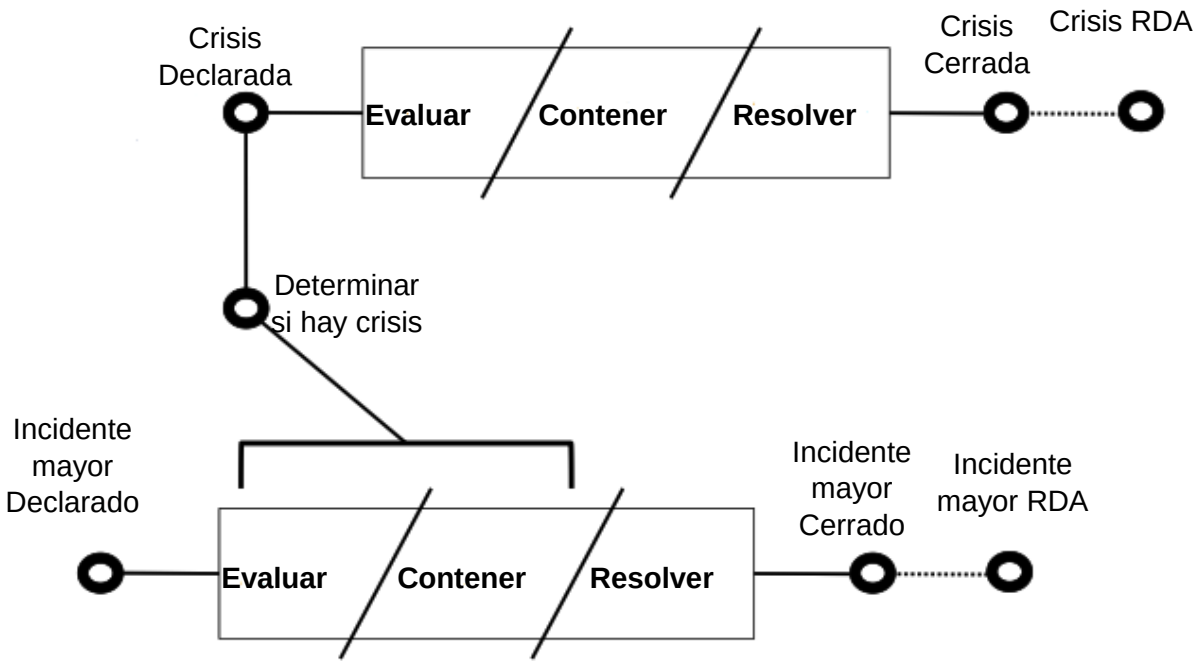
- Lucas, J. Moeller, B. (2004). The Effective Incident Response Team. Boston, MA. Addison-Wesley Professional
- Ballen, M, Pulido, R, Zuñiga, F (2007). *Abordaje hermenéutico de la investigación cualitativa. Teorías, procesos, técnicas.* Medellin, Colombia. Teoría del Color.
- Gomez, A. (2011). Gestión de Incidentes de Seg. Informática (MF0488_3). España. Starbook Editorial, S.A.
- Fonseca, O. (2013). *Sistema de control interno para organizaciones.* Lima, Perú Publicidad & Matiz.
- S. Davidson, Managing the message: Communication and media management in a security crisis. EISF, 2013. Recuperado de:https://www.eisf.eu/wp-content/uploads/2014/09/1140-Davidson-2013-Managing-the-Message-Communication-and-media-management-in-a-security-crisis.pdf
- Hernández, R. (2014). *Metodología de la investigación.* México, D.F. McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.
- Bernard, P. (2014). *IT Service Management Based on ITIL® 2011*. Cocobook Editorial.
- Ramos, A. (2014). *Gestión del Servicio en el Sistema Informático*. Madrid, España. RA-MA Editorial.
- Chicano, E. (2015) *Gestión de incidentes de seguridad informática. IFCT0109*. Malaga, España. IC Editorial.
- EC-Council, (2016). Computer Forensics: Investigation Procedures and Response (CHFI). Boston, MA. Cengage Learning.
- Nieloroja (July 20, 2017). ISO IEC 27035-3. kupdf.net. Recuperado de: https://kupdf.net/download/iso-iec-27035 3_59700291dc0d60b33ca88e7e_pdf
- Schreider T. (2017). Building Effective Cybersecurity Programs: A Security Manager's Handbook. Connecticut USA. Kristen Noakes-Fry (Editor).

- Schnepp, R. Vidal, R., Hawley, C. (Julio 2017) Incident Management for Operations. California. O'Reilly Media.
- Thompson, E. (2018). Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from incidents. Illinois, USA. Apress.
- Stallings W. (2018). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley
- Procedimientos de Gestión de Incidentes de Seguridad (GDPR) (2018). Gonvarri Steel Services. Recuperado de : https://www.gonvarristeelservices.com/wp-content/uploads/2018/10/Procedimiento-de-Gesti%C3%B3n-de-Incidentes-de-Seguridad-GDPR.pdf
- Establishing Incident Management for Your Service. (s.f). Stanford University. Recuperado de: https://uit.stanford.edu/service-management/toolkit/incident
- DICT Computer Emergency Response Team (CERT) Manual. (s.f). Republica de Philipinas. Recuperado de: https://www.ncert.gov.ph/cert-manual/dictcertmanual.pdf.

X. Anexos

Anexo 1: Flujo de trabajo de incidentes mayores y situaciones de crisis

***RDA** (Revisión después de la acción)



Anexo 2: Horas laborales vs fuera de horas laborales.

Los deberes del Coordinador de incidentes mayores se manejan por separado entre el horario laboral y después del horario laboral.

Horario Laboral: entre las 8:00 a.m. y las 5:00 p.m. De lunes a viernes (exceptuando días feriados).

Fuera del horario laboral: entre las 5:01 p.m. y de 7:59 a.m. de lunes a viernes y todo el día los fines de semana y días feriados.

Responsabilidades fuera de horario

- La semana de guardia las horas comienzan y terminan el viernes a las 5:00 p.m.
- La responsabilidad fuera del horario laboral de atención se programa semanalmente.
- La rotación de personal se mantiene en el Calendario del coordinador de incidentes.

La persona activa de guardia después de las horas laborales es responsable de cambiar el número de transferencia de llamadas de Gestión de incidentes a la siguiente persona programada cuando su rotación de guardia finalice el viernes.

Si desea cambiar los períodos de guardia, debe comunicarse con el Propietario del proceso antes de su horario de rotación para que se pueda actualizar el calendario de guardia.

Anexo 3: Equipo de guardia

Tenga el siguiente equipo disponible y listo para su rotación fuera de horario:

Ordenador portátil

- Punto de acceso a Internet LAN-WAN (si no tiene uno, consulte al área de Base de datos y Sistemas operativos para brindar acceso).
- Informes del turno de guardia.
- Manual de referencia del coordinador de incidentes (Manual del coordinador de incidente).

Todo el personal de guardia debe guardar los números de los turnos de todos los grupos DIS en sus teléfonos.

Anexo 4: Compensación

Según la política de viáticos de la Dirección Financiera DGI, sobre turnos de vigilancia, los empleados no exentos reciben una compensación de C$500 por semana por las tareas de guardia después del horario de atención.

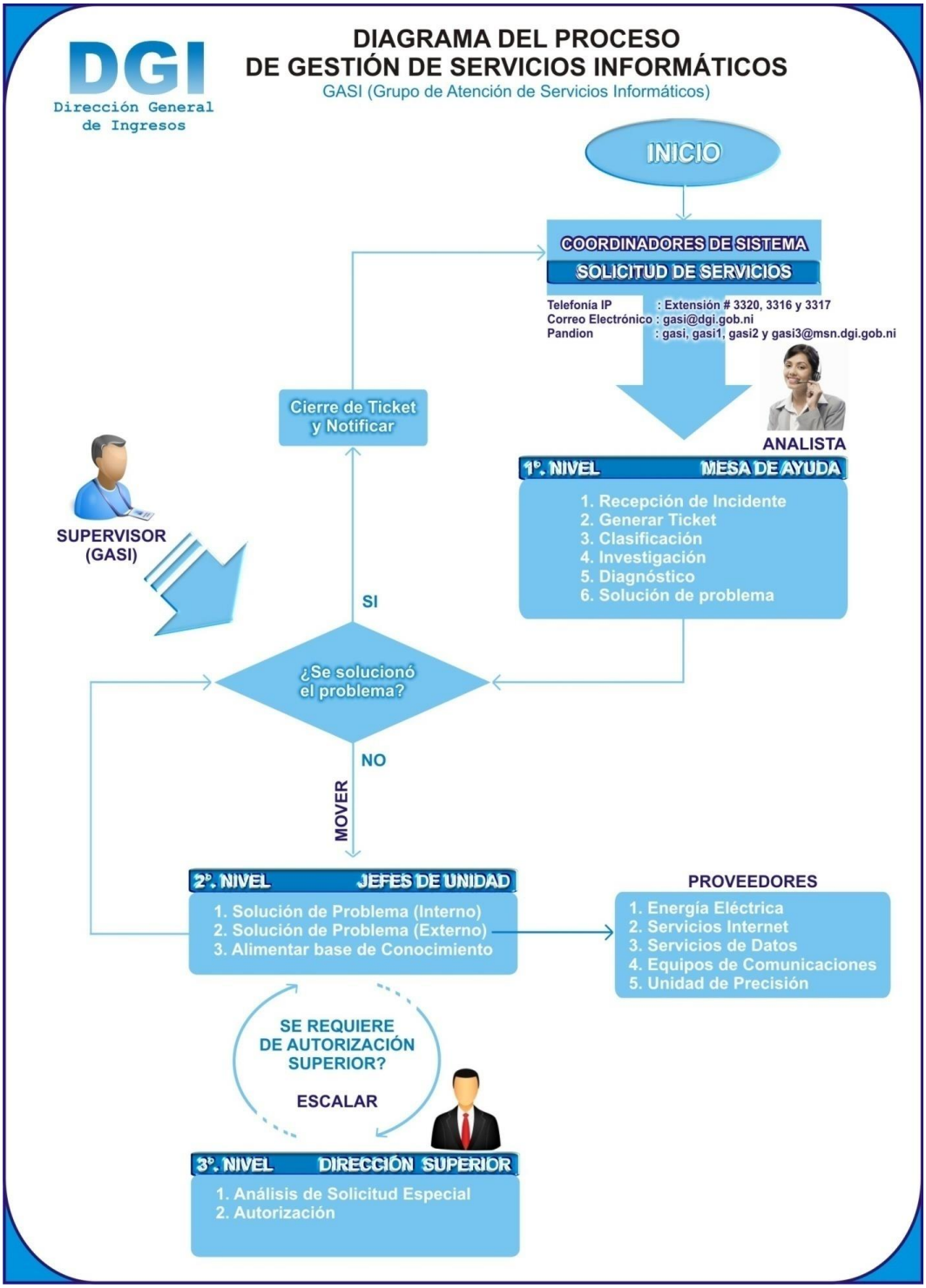
Los empleados exentos son igualmente reembolsados con un estipendio salarial. Los formularios de reembolso y las instrucciones están disponibles con el personal de la Dirección Financiera.

Anexo 5: Información de contacto de guardia

Todos los equipos técnicos de la DIS tienen números de contacto dedicados para la respuesta a incidentes mayores 24x7. Durante el horario comercial, su llamada debe ser devuelta dentro de los 15 minutos. Durante horas extras, el personal de servicio técnico del grupo técnico debe responder a su página en un plazo de 30 minutos. Si el personal de guardia no devuelve su llamada dentro del tiempo designado, el Coordinador de incidentes debe pasar al Administrador de recursos técnicos de guardia apropiado. Todo el personal de guardia debe guardar los números de llamada de todos los grupos DIS-DGI en sus teléfonos.

La lista de números de contacto de guardia está disponible y actualizada en las siguientes ubicaciones http://directorio.dgi.gob.ni.

Anexo 6: Diagrama de proceso de servicios informáticos mesa de ayuda (GASI)



Anexo 7: Plantillas de notificación por correo electrónico

Notificaciones internas

En el caso de que GASI no esté disponible, envíe notificaciones manuales por correo electrónico interno desde la cuenta de correo alertadis@dgi.gob.ni

Use las siguientes plantillas para notificaciones internas.

Tipo: NUEVO INCIDENTE MAYOR

Use esta plantilla para la notificación INICIAL de un incidente mayor, a menos que el incidente ya esté resuelto. Para los incidentes resueltos antes de la Notificación inicial.

DE: Gestión de incidentes DIS (alertasdis@dgi.gob.ni)

PARA: *********@dgi.gob.ni

ASUNTO: <Nombre del servicio> interrumpido o degradado

Estado del incidente mayor: Nuevo

Categoría de incidente mayor: [1 - Evaluar / Impacto limitado] O [2 - Contener / Posible solución] O [3 - No conocido

Solución / Impacto significativo:

Tiempo informado:

Inicio de incidentes:

Impacto en el usuario / negocio:

Servicios afectados:

Puente de Conferencia de Incidentes Mayores: 866-890-3820 38793366 #

Grupo (s) Responsable (s):

Grupo de propietarios de servicios:

Acciones actuales:

[Tu nombre]

Gestión de Incidentes DIS

12345678

**** SOLO PARA USO INTERNO DIS *****

Tipo: ACTUALIZACIÓN

Use esta plantilla para la notificación de ACTUALIZACIÓN interna cuando ya se haya enviado una notificación inicial. Si se resuelve un incidente importante antes de que se envíe la notificación inicial, utilice la plantilla Resuelto tras la notificación.

DE: Gestión de incidentes DIS (alertasdis@dgi.gob.ni)

PARA: *********@dgi.gob.ni

ASUNTO: ACTUALIZACIÓN: <Nombre del servicio> interrumpido o degradado

Estado del incidente mayor: actualización

Categoría de incidente mayor: [2 - Contener / Posible solución] O [3 - Sin solución conocida / Impacto significativo] Tiempo informado:

Inicio de incidentes:

Actualizar:

Impacto en el cliente / negocio:

Servicios afectados:

Puente de Conferencia de Incidentes Mayores: 866-890-3820 38793366 #

Grupo (s) Responsable (s):

Grupo de propietarios de servicios:

Acciones actuales:

[Tu nombre]

Gestión de Incidentes DIS

12345678

***** SOLO PARA USO INTERNO DIS *****

Tipo: RESOLUCIÓN O RESUELTO EN LA NOTIFICACIÓN

Use esta plantilla para la notificación interna de RESOLUCIÓN.

DE: Gestión de incidentes DIS (alertas@dgi.gob.ni)

PARA: **********@dgi.gob.ni

ASUNTO: <Nombre del servicio> Restaurado

Estado del incidente mayor: resuelto

Categoría de incidente mayor:

Tiempo reportado:

Inicio del incidente:

Fin del incidente:

Duración: # horas # minutos

Acciones de resolución:

Próximos pasos:

Impacto en el usuario / negocio: Servicios afectados:

Grupo (s) responsable

Grupo de propietarios de servicios:

[Tu nombre]

Gestión de Incidentes DIS

12345678

***** SOLO PARA USO INTERNO DIS *****

Anexo 8: Cambios de emergencia fuera del horario de atención

El Coordinador de incidentes después de las horas de trabajo también es responsable de la notificación de los cambios de emergencia (inmediatos). En caso de un cambio inmediato fuera del horario de atención, el representante del grupo técnico llamará al Coordinador de incidentes de guardia.

La implementación de cambios proporcionará la siguiente información:

- ¿Qué trabajo se está realizando?
- ¿El director del grupo técnico ha dado su aprobación?
- ¿Qué impacto tendrán los cambios en los servicios?
- ¿Se interrumpirán los servicios?
- ¿Cuándo comenzará y terminará el trabajo?

NOTA: El coordinador de incidentes de guardia solo es responsable de las comunicaciones, no de la aprobación. El proceso de gestión de cambios de DIS permite la aprobación del director de los cambios de emergencia inmediatos después del horario de atención.

Anexo 9. Tipo Notificación de cambio de emergencia - IMPACTO EXTERNO

Si el cambio tendrá un impacto externo, publique una notificación web en www.dgi.gob.ni

Use esta plantilla para la notificación interna de MANTENIMIENTO.

DE: Mesa de ayuda (gasi@dgi.gob.ni)

PARA: **********@dgi.gob.ni

ASUNTO: <Nombre del servicio> MANTENIMIENTO

Nombre de mantenimiento: [Servicio] Mantenimiento urgente

Detalles de mantenimiento: para [proteger, restaurar] servicios críticos, DIS realizará un mantenimiento urgente a [nombre del servicio]. El acceso a [la red, aplicaciones o servicios específicos] estará [no disponible, interrumpido brevemente] durante este evento.

Hora de inicio del mantenimiento: ingrese la fecha y hora proporcionadas

Hora de finalización del mantenimiento: ingrese la fecha y hora proporcionadas

Alertar a los usuarios suscritos a: ver los servicios que se verán afectados por este cambio de emergencia

Estado en "En progreso" al comienzo del período de mantenimiento c.

Estado en "Completado" al final del período de mantenimiento

[Tu nombre]

Gestión de Incidentes DIS

12345678

***** SOLO PARA USO INTERNO DIS *****

Anexo 10. Plantilla: Correo Alerta DIS

Asunto: [DIS-Alertas] INC ######## - Descripción

Estado del incidente mayor:

Categoría:

Tiempo reportado:

Inicio de incidentes:

Impacto en el negocio:

Servicios afectados:

Puente de Conferencia de Incidentes Mayores: 3447 #

** Se esperan representantes de grupos de propietarios técnicos y de servicio en el puente de llamada para evaluación del incidente dentro de los 15 minutos de la alerta DIS.

Grupo (s) responsable (s):

Grupo de propietarios de servicios: Gestión de servicios de TI (ITSM)

Actualizaciones de estado: Estado del servicio DIS http://servicios.dis.dgi.gob.ni

Acciones actuales:

Nombre del coordinador de incidentes

Gestión de Incidentes DIS

12345678

Anexo 11. Encuestas a los Directores DIS.

Preguntas Generales	Si	/ No	/ En parte
¿Cuenta la DIS con una política sobre gestión de incidentes de seguridad de la información?	☐	☐	☐
¿Se dispone de procedimientos de gestión de incidentes en la DIS?	☐	☐	☐
¿Los procedimientos de gestión de incidentes incluyen un árbol de Comunicaciones?	☐	☐	☐
¿Los procedimientos de gestión de incidentes abordan los incidentes que son falsos?	☐	☐	☐
¿Se forma al personal sobre la gestión de incidentes o crisis?	☐	☐	☐
¿La DIS utiliza un sistema en línea para gestionar los incidentes?	☐	☐	☐
¿Utiliza la organización un programa de procesamiento de textos u hojas de cálculo como base de su sistema de gestión de incidentes?	☐	☐	☐
¿Se ha convenido en un procedimiento de comunicaciones Relativas a incidentes con los proveedores?	☐	☐	☐
Recopilación de la información sobre incidentes	**Si**	**/ No**	**/ En parte**
¿Existe una definición de la DIS del término "incidente"?	☐	☐	☐
¿Utiliza la DIS categorías definidas para describir distintos tipos de incidentes?	☐	☐	☐
¿Existe una plantilla de informe de incidentes?	☐	☐	☐
¿Existe un procedimiento para reuniones posteriores sobre incidentes resueltos?	☐	☐	☐
¿Existe una base del conocimiento para la información recabada?	☐	☐	☐
¿Recopila información la DIS sobre incidentes externos (es decir, los que no tienen repercusiones en la DIS)?	☐	☐	☐
Reportes sobre incidentes	**Si**	**/ No**	**/ En parte**
¿Existe un procedimiento para reportar incidentes?	☐	☐	☐
¿Existen directrices de apoyo a la plantilla de informe de incidentes?	☐	☐	☐
¿Existe reportes de incidentes para cada oficina?	☐	☐	☐
¿Existe una lista de contactos disponible?	☐	☐	☐
¿Se aplica un sistema de registro de incidente?	☐	☐	☐
¿Se registran daños y pérdidas en infraestructura o equipos?	☐	☐	☐
¿Se registran amenazas verbales, escritas o virtuales a la DIS?	☐	☐	☐
¿Se registran las trabas administrativas?	☐	☐	☐
¿Los sistemas están seguros en todos los ámbitos? ¿Los datos están seguros?	☐	☐	☐
Análisis de la información sobre incidentes	**Si**	**/ No**	**/ En parte**
¿Existe una plantilla para reportar incidentes que ofrezca orientación sobre la información que ha de recopilarse a efectos analíticos (por ejemplo, 4 horas después del evento)?	☐	☐	☐
¿Alguien se encarga de analizar los incidentes?	☐	☐	☐
¿Alguien se encarga de analizar / verificar los resultados de los análisis?	☐	☐	☐
¿Se forma al personal para mejorar sus destrezas analíticas (en materia de seguridad)?	☐	☐	☐
¿Se dispone de un sistema para mapear (Por ejemplo: mediante una hoja de cálculo) y analizar incidentes?	☐	☐	☐
¿Se consultan fuentes externas (partes interesadas o información) durante el análisis de incidentes?	☐	☐	☐
Compartir información sobre incidentes	**Si**	**/ No**	**/ En parte**
¿Existen políticas generales sobre clasificación de la información en la DIS?	☐	☐	☐
¿Se dispone de políticas sobre comunicaciones internas?	☐	☐	☐
¿Existe una política sobre comunicaciones externas?	☐	☐	☐
¿La DIS utiliza las redes sociales para comunicaciones generales?	☐	☐	☐
¿La DIS tiene vínculos firmes con partes interesadas de medios?	☐	☐	☐
¿Las comunicaciones internas suelen ser verbales o por escritas?	☐	☐	☐
¿Las comunicaciones externas suelen ser verbales o por escrito?	☐	☐	☐

¿Existe un documento de traspaso para referentes que incluya la información sobre incidentes?	☐	☐	☐
¿Se ha formado al personal para compartir información de incidentes y las políticas de la DIS?	☐	☐	☐
Uso de la información sobre incidentes	**Si**	**/ No**	**/ En parte**
¿Se ha nombrado a alguien para que se encargue de las acciones de seguimiento (a medio plazo)?	☐	☐	☐
¿Existe una comunicación de seguimiento un mes después del incidente?	☐	☐	☐
¿Existe una comunicación de seguimiento tres meses después del incidente?	☐	☐	☐
¿La DIS hace seguimiento de que se apliquen las lecciones aprendidas?	☐	☐	☐
¿La DIS hace análisis cuantitativo?	☐	☐	☐
¿La DIS hace análisis cualitativo?	☐	☐	☐
¿La DIS dispone de un sistema para hacer análisis de datos cuantitativos sobre incidentes?	☐	☐	☐
¿Se celebran reuniones en la DIS para presentar las tendencias de seguridad de la información al personal?	☐	☐	☐