UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:

ESTUDIO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA JARDÍN AZUAYO

AUTOR:

MARCO ORLANDO REAL ARÉVALO

DIRECTOR:

JOSÉ LUIS AGUAYO MORALES

CUENCA – ECUADOR

2023

Autor:

Marco Orlando Real Arévalo.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
Ingeniero en Informática.
Magister en Ciencias de la Computación. Mención Networking.
mreala1@est.ups.edu.ec

Dirigido por:

José Luis Aguayo Morales
Ingeniero en Electrónica y Telecomunicaciones.
Magister en Ciberseguridad.
Magister en Sistemas Informáticos Educativos.
Magister en Redes de Comunicación.
jaguayo@ups.edu.ec

DEDICATORIA.

Las personas como la vida somos pasajeras y ambas nos dan enseñanzas, muchas personas han pasado y siguen pasando por mi vida, a algunas ya ni los veo, a otras muy frecuentemente y otras se están alejando… quiero dedicar este trabajo a mis hijos de quienes estoy muy orgulloso; a mis padres que todavía viven y me acompañan, no he sido el hijo que merecen y, sin embargo, siempre están ahí.

AGRADECIMIENTO.

A Dios, por haberme imaginado, no he sido un buen interprete de su partitura y; sin embargo, me acompaña siempre; a mis padres por ser incondicionales, a mis hijos por comprender, por brindarme su sonrisa y cariño, siempre estaré orgulloso de ustedes, gracias.

Este agradecimiento no estaría completo si no expresara un grato reconocimiento a cada uno de los maestros y profesores de esta maestría, por su esfuerzo y dedicación y desde luego a la Universidad Politécnica Salesiana por ponerse a la vanguardia de las necesidades de la sociedad y de las empresas e instituciones, gracias.

Tabla de Contenido

Tabla de Ilustraciones

Estudio para la Implementación del sistema de Gestión de Incidentes de seguridad de la información para la Cooperativa Jardín Azuayo

Autor:

MARCO ORLANDO REAL AREVALO

Resumen

Este estudio ha sido desarrollado con la finalidad de proveer a la Cooperativa de Ahorro y Crédito Jardín Azuayo una herramienta que permita anticiparse a los eventos y que estos no se conviertan en incidentes de seguridad de la información; para ello se ha tomado en consideración el entorno en el que una institución de su estilo se desenvuelve y la necesidad de estar a la vanguardia; acercar sus servicios y mantenerse competitivo.

En este estudio se analizar algunos estándares, marcos de trabajo, etc., que sirven y aportan a la gestión de incidentes, estos son COBIT, ITIL, ISO 27035 y NIST, así mismo, también se toma en cuenta regulaciones del sector que se encuentran vigentes y que deben ser considerados al momento de la implementación del sistema de gestión de incidentes como la resolución R 002 de la SEPS, pues, no se trata de seleccionar uno u otro; porque de hecho la orientación de cada uno es diferente y lo que hacen respecto de los incidentes es proveer una serie de "recomendaciones" que han sido probadas y validadas por las industrias alrededor del mundo y que desde su óptica aportan en la prevención de incidentes; lo que pretende este estudio, es que exista un alineamiento entre estos frameworks, mejores prácticas y estándares, ya que en la cooperativa están siendo usados para los diferentes ámbitos de su gestión y gobierno.

Los servicios electrónicos de Jardín Azuayo se alinean a su misión, cuando se habla de cercanía y eso se logra a través de una herramienta imprescindible como es el internet y a través de esta la cooperativa llega con un conjunto de servicios electrónicos como Página web transaccional, banca móvil, corresponsalías, cajeros automáticos, puntos de atención virtual y otros servicios físicos tanto de crédito como de ahorro).

La propuesta organiza la gestión de incidentes, sus responsables, los eventos a seguir, cumpliendo las regulaciones y además es factible de implementar por su retorno de inversión de seguridad.

Palabras clave:
Incidentes, estándares, gestión, marcos de trabajo, mejores prácticas, COBIT, ITIL, ISO, NIST.

ABSTRACT

This study has been developed with the purpose of providing the Jardín Azuayo Savings and Credit Cooperative with a tool that allows them to anticipate events and prevent them from becoming information security incidents. To achieve this, the environment in which an institution like theirs operates and the need to stay ahead of the curve were taken into consideration, in order to bring their services closer to customers and remain competitive.

This study analyzes some standards, frameworks, etc., that serve and contribute to incident management, such as COBIT, ITIL, ISO 27035, and NIST. Additionally, regulations that are currently in force and must be considered when implementing an incident management system, such as SEPS Resolution R 002, are also taken into account. Each of these resources provides a set of tried and tested recommendations for incident prevention, which are different from one another. The aim of this study is to promote alignment between these frameworks, best practices, and standards, as they are being used by the cooperative for various aspects of their management and governance.

Jardín Azuayo electronic services align with their mission of customer proximity or closeness, which is achieved through the indispensable tool of the internet. Through the internet, the cooperative offers a set of electronic services, such as transactional web pages, mobile banking, correspondents, ATMs, virtual service points, and physical services for both savings and credit.

The proposal outlines incident management responsibilities and how to handle events in accordance with regulations, while also being feasible to implement due to its security return on investment.

Palabras clave:
Incidents, standards, management, frameworks, COBIT, ITIL, ISO, NIST.

1. Introducción

Cada día son más las empresas de cualquier índole y orientación que dependen casi totalmente de la tecnología, también es cada vez mayor la necesidad de conectar servicios al internet, ya sea como parte de un estratégica de comercialización y ventas o como parte de brindar facilidades de acceso a sus usuarios y como el caso de la cooperativa que tiene como misión promover la inclusión financiera de sus socios a través de sus servicios como banca virtual, aplicaciones móviles, botón de pago, entre otros y productos financieros como los de crédito en general y de ahorros, pólizas de acumulación, etc., pues la Cooperativa Jardín Azuayo, no solo promueve el uso, accesibilidad y agilidad sobre sus productos, sino que ahora es una prioridad el que estos productos y servicios lleguen con las mayores garantías que la tecnología, los procesos y los recursos pueden ofrecer. Así pues, la tecnología incluso la más actual tiene riesgos intrínsecos que se convierten en vulnerabilidades por ende en puertas de entrada para cualquier tipo de ataque, los procesos en cambio son la formas de como las personas operan y están provistas de entradas y salidas en todo este flujo siempre debe estar considerado la seguridad.

Por ello, los esfuerzos que como institución se hagan y se puedan hacer redundarán en seguridad para sus socios permitiendo generar confianza sobre los servicios y productos que tanto en las captaciones (Ahorro programado, Ahorros a la Vista, Póliza de acumulación) y colocaciones (Crédito de consumo, crédito para vivienda, avances en efectivo, crédito ordinario) se ofrecen.

La gestión de incidentes de seguridad de la información es una forma de prever y anticiparse a cualquier situación disruptiva que vulnere estas garantías, para ello es necesario prepararse y organizarse para atender las alertas que los controles pueden mostrar.

Es importante que la gestión de incidentes se incorpore de forma integral a los procesos de la cooperativa, junto con la estructura del SGSI y sus controles de esta manera se visibilizará de mejor manera a la alta gerencia.

Cada vez son más frecuentes los ataques a las infraestructuras críticas y sus servicios. [1], uno de los sectores más afectados es el financiero en el que se desenvuelve la cooperativa, por ello, el monitoreo de los controles establecidos, así como la atención que se dé a las alarmas o alertas de seguridad es primordial y necesario.

La Cooperativa debe estar prepara para realizar una transición de acuerdo con la situación, es decir, basada en estados donde se pueda establecer la operación normal y de acuerdo con el monitoreo de las alertas se puedan reconocer eventos críticos y dar atención a un posible compromiso de los servicios institucionales.

2. Determinación del Problema

La Cooperativa Jardín Azuayo cuenta desde el año 2015 con un Sistema de Gestión de Seguridad de la Información (SGSI); sin embargo, por sí solo este sistema no evita que se den o susciten algunos eventos que pueden derivar en un incidente y esto pueda afectar la operación normal de ciertos usuarios o departamentos, peor aún, no se puede evitar que un incidente pueda afectar la continuidad de las operaciones y servicios institucionales que como ente financiero podría derivar en serios problemas, que más allá de lo legal puede representar un daño reputacional grave; que la cooperativa pueda responder de manera adecuada a este tipo de eventos es el objetivo de la implementación del Sistema de Gestión de Incidentes de Seguridad de la Información, además hay que comprender que los incidentes pueden ser de diferente índole; entonces deberíamos preguntarnos ¿de dónde puede derivar un incidente?, ¿a qué se identifica como incidente? ¿quién o quiénes deben responder estos incidentes?, ¿está la cooperativa preparada para los eventos e incidentes que el entorno en el que se desenvuelve le plantea?; son algunas de las preguntas que este estudio debe responder de forma clara y concreta para que no quede duda a la administración respecto de la necesidad de contar con un sistema de gestión de incidentes.

Las industrias y/o empresas ecuatorianas al igual que el mundo entero al estar inmersos en la tecnología y conectados al internet a través de los servicios que se pueden ofrecer, está sujeta a una serie de ataques cada vez más letales que han evidenciado que por más que las instituciones realicen grandes inversiones simple y sencillamente parecen no ser suficientes porque al fin sea la tecnología que sea incluso la más actual siempre estará propensa a fallos y vulnerabilidades que los atacantes aprovechan de ahí se justifica la necesidad que la cooperativa Jardín Azuayo sea capaz de responder apropiadamente ante un evento disruptivo.

Alrededor del mundo se ha comprendido que el internet es un medio hostil; sin embargo, esto no puede frenar a las instituciones como la cooperativa en su

propósito de facilitar el acceso a sus servicios financieros de crédito y ahorro en cualquier parte del mundo, de eso se trata en la actualidad; no puede una empresa del sector que sea estar desconectado del internet y mucho menos la cooperativa que como parte de sus objetivos estratégicos garantiza el acceso, facilidad y cercanía de los servicios, entonces es totalmente necesario que se responda adecuadamente a los posibles amenazas que trae consigo este medio hostil.

Integrar la gestión de incidentes al Sistema de Gestión de Seguridad de la Información permitirá dar respuesta de manera efectiva y estructurada a los posibles eventos e incidentes que se puedan suceder.

Al finalizar este estudio se planteará las oportunidades y deficiencias que puede ofrecer la implementación del sistema de gestión de incidentes para los socios, directivos y colaboradores, pero sobre todo hacer que las deficiencias sí bien no pueden desaparecer, al menos disminuir los efectos adversos sobre la pérdida de la confidencialidad, integridad y disponibilidad de la información que la cooperativa gestiona.

3. Estado del Arte.

La Cooperativa Jardín Azuayo viene teniendo un alto nivel de crecimiento desde su conformación; crecimiento que exige solidez en la estructura organizativa, en el modelo de gestión y sobre todo en el desarrollo y calidad de sus servicios.

Por consiguiente, la estructura de la Cooperativa de Ahorro y Crédito "Jardín Azuayo" es un medio de gestión efectivo que refuerza la coherencia y modelo de administración mediante la definición clara de su configuración organizativa. Este se realiza para garantizar el logro de su propósito, visión y metas estratégicas, en línea con su filosofía institucional, valores y principios cooperativos, tal cual se encuentra descrito en el Manual Orgánico Funcional, MA-TAL-01, versión 6.9 del 30 de septiembre de 2022, (documento de uso interno).

Esta estructura de organización tiene como base una administración organizada y participativa, cuyo objetivo principal es consolidar la coordinación interna y crear un clima comunicativo fluido, con el fin de ofrecer una atención integral y de excelencia a los usuarios, socios y clientes.

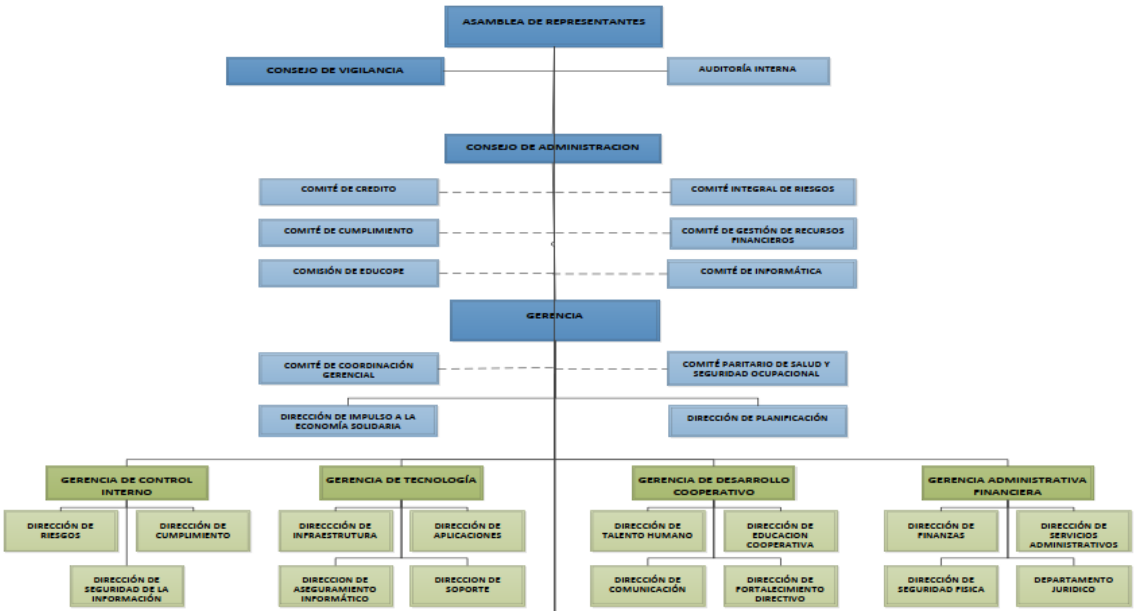


Gráfico 1, Organigrama Cooperativa Jardín Azuayo - Manual Orgánico Funcional, MA-TAL-01, versión 6.9

Esta estructura organizativa ha permitido que la cooperativa tenga un posicionamiento importante en el sector cooperativo, de ahí la importancia de gestionar adecuadamente los recurso y de ofrecer servicios confiables y seguros, es por eso que la cooperativa decidió implementar un Sistema de Gestión de Seguridad de la Información donde como parte de este proceso y para una adecuada gestión de los riesgos se identificaron los activos de información de cada uno de los procesos críticos que la institución tiene.

Como es conocido, para que un SGSI sea efectivo y sobre todo como un requisito para quienes se alinean a la serie ISO 2700X es la identificación de los denominados activos de información (NTE INEN-ISO/IEC 27000:2018 – Descripción General y Vocabulario: "conocimiento o datos que tiene valor para la organización"), una vez identificados los activos de información es necesario de acuerdo a su criticidad establecer controles y mitigar sus riesgos por ello es necesario realizar un análisis de riesgos, mismo que permitirá realizar un adecuado tratamiento para ello se ha decidido adoptar la norma NTE INEN-ISO/IEC 27005:2017 - Gestión de Riesgos en la Seguridad de la Información y que busca preserva la Confidencialidad, Integridad y Disponibilidad de la información (NTE INEN-ISO/IEC 27000:2018 – Descripción General y Vocabulario: "La seguridad de la información incluye tres dimensiones principales: confidencialidad, integridad y disponibilidad") que es almacenada, procesada y distribuida.

Hoy en día, las tecnologías de la información son fundamentales para el desenvolvimiento de la sociedad, en especial para el funcionamiento de las empresas e industrias; los procesos, la cadena de producción, la atención al cliente, todo depende de la tecnología e incluso hemos vuelto "inteligentes" a los electrodomésticos; ya nadie concibe la vida actual sin tecnología; entonces imaginar que un evento indeseado, por ejemplo no permite acceder a los ahorros porque la institución financiera (banco, cooperativa) no tiene sus servicios bancarios disponibles; puede representar una gran preocupación para sus clientes, si este evento demora muchos minutos, o varias horas, o peor aún varios días, puede llevar a la debacle para la institución, ya que las pérdidas se dimensionan por hora, por

día, sumando a esto el nerviosismo de los clientes o los usuarios, junto con el fenómeno actual donde no es necesaria la noticia sino solo con los “influencer” y las redes sociales donde se especula o desinforma es una mezcla potencialmente peligrosa al que las instituciones deben buscar la forma de responder de forma efectiva y adecuada de ahí que alrededor del mundo se han diseñado estándares y mejores prácticas orientadas a la respuesta a incidentes denominados “Gestión de incidentes de seguridad de la información”, como lo describe la norma “ISO/IEC 27035: information technology, security techniques – information security incident mangement (tecnologías de información, técnicas de seguridad – sistema de gestión de incidentes de seguridad)”.

Los estados vienen preocupándose por la seguridad de la información al menos desde mediados del siglo anterior, todo a partir de la paranoia bélica y a partir de entender que la información es más valioso que el mismo oro o petróleo y ya para la época actual se ha visto que las industrias, empresas o instituciones han implementado estrategias para proteger la información y lo que han hecho ciertos estados es tomar esas experiencias y convertirlas en estándares que se han convertido en referencias para el mundo entero; de ahí que instituciones como el Institute Standard Organization (ISO por sus siglas en inglés), han diseñado un estándar orientado el cuidado y preservación de la información denominado: ISO/IEC 27001: information technology, security techniques – information security management systems - Requirement, el National Institute of Standards (ISO/IEC 27001: tecnologías de información, técnicas de seguridad – Sistema de Gestión de Seguridad de la Información - Requisitos) de esta misma manera otras instituciones también han desarrollado sus propios estándares de seguridad como el National Institute of Standards Technology (NIST por sus siglas en inglés), entre otros que han abordado el tema de la gestión de seguridad para atender la preocupación de los sectores con el fin de tratar adecuadamente la protección de la información.

Cada vez que el ser humano o las industrias han ido dependiendo de la tecnología, también han ido apareciendo grupos de individuos que han visto en la tecnología una oportunidad para enriquecerse a partir de aprovechar sus vulnerabilidades y

más aún cuando al parecer es más fácil atacar que defenderse; pues las instituciones - empresas pueden invertir grandes cantidades de dinero en tecnología de seguridad y esta, al mismo tiempo no es suficiente para atender completamente a los problema de seguridad, porque la dependencia del factor humano y la fragilidad de su comportamiento en ciertos momentos ponen en riesgo la disponibilidad, integridad y confidencialidad de los servicios.

Ante esta conjunción de eventos, surgen los problemas para las empresas y es donde se debe trabajar de forma constante y sostenida, para crear conciencia y conocimiento sobre el rol de las personas en el ámbito de la seguridad; de ahí que la gestión de incidentes se hace necesario e imprescindible y motiva el desarrollo de este trabajo.

Como se ha indicado anteriormente en el mundo existen una serie de estándares y mejores prácticas relacionados con la gestión de incidentes e incluso algunos marcos de trabajo (frameworks) orientados a la gestión de tecnologías de la información como COBIT (APO13: Gestión de la Seguridad, DSS04: Gestión de la Continuidad, DSS05: Gestión de Servicios de Seguridad) e ITIL (Sistema de Valor del Servicio - SVS) para la gestión de la mesa de ayuda han incluido en su últimas actualizaciones la relación con la gestión de incidentes de seguridad de la información, en este trabajo es necesario analizar cada una de ellas ya que siendo La Cooperativa Jardín Azuayo una institución que busca brindar a sus socios, clientes y usuarios servicios de calidad se alinee con los estándares relacionados y es menester que estos se ajusten a su gestión y además le permita dar cumplimiento a normativas y leyes aplicables.

3.1 ESTÁNDARES PARA LA GESTIÓN DE INCIDENTES

La normas y marcos de trabajo orientadas a la seguridad de la información, así como los controles por si solos no garantizan la protección completa de la información,

de las infraestructuras, de las redes de comunicaciones y de los sistemas de información.

Hay que reconocer que aún la tecnología más moderna y eficiente está expuesta a vulnerabilidades que puede exponer fuertemente la información que sustentan derivando en incidentes de seguridad de la información, de ahí la necesidad que las empresas de todo tipo o sector implementen de forma adecuada un sistema de gestión de seguridad de la información e incidentes basado en estándares o mejores prácticas de general aceptación.

3.1.1 ITIL

La Biblioteca de Infraestructura de Tecnologías de información es una guía de buenas prácticas que desde la versión 3 en su libro de Operación del Servicio ya habla de Administración de Incidentes y en su última versión (4) incorpora un proceso de gestión de incidentes (Incident Management) que promete una adecuada operación de una empresa o institución garantizando a sus clientes tanto internos y externos que sus servicios estarán disponibles ante cualquier evento o incidente.

ITIL define un incidente como "*una interrupción no planificada de un servicio, o reducción en la calidad de un servicio*", el objetivo del proceso de gestión de incidentes en ITIL es reducir el impacto adverso de los incidentes a través de la restauración de la operación normal del servicio en el menor tiempo posible, descrito dentro del Sistema de Valor del Servicio (SVS).

En la metodología ITIL se describe la gestión de incidentes dentro de lo que se denomina Sistema de Valor del Servicio (SVS) y plantea como objetivo restaurar en el menor tiempo posible cualquier interrupción o retraso que afecte la calidad del servicio, desde luego que no haya sido planificada cuyo objetivo es minimizar el impacto de las operaciones y su premisa es evitar que los incidentes vuelvan a ocurrir. En ITIL se habla de Problema como la causa subyacente de un incidente; la gestión de problemas funciona en estrecha colaboración con la gestión de incidentes, pero no es lo mismo.

La gestión de incidentes tiene como objetivo restablecer los servicios rápidamente, generalmente mediante la implementación de soluciones temporales, mientras que la gestión de problemas se enfoca en examinar las causas subyacentes y prevenir futuros incidentes.

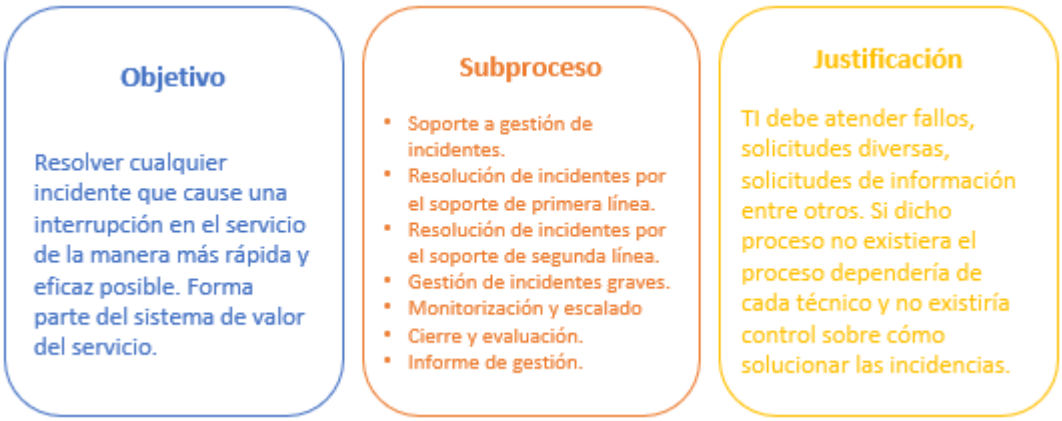


Gráfico 2, ITIL, Objetivos, Subproceso, Justificación - Sistema de Valor del Servicio (SVS)

3.1.2 COBIT

Se trata de un marco de trabajo (framework) para el gobierno y la gestión de las tecnologías de información orientado a todo tipo de empresa. COBIT ha ido evolucionando desde haber sido concebido para la auditoría de TI hasta involucrar a la gerencia en la gestión de las tecnologías; independiente de lo que sucede en la empresa. En este contexto COBIT provee herramientas para la gestión y el gobierno haciendo una clara distinción entre estos dos términos (COBIT 2019 Governance and Management Objectives).

El gobierno asegura que las necesidades de las partes interesadas se toman en cuenta para determinar los objetivos empresariales a través de la priorización en la toma de decisiones, su desempeño y cumplimiento son monitoreados en base a los objetivos definidos, (COBIT 2019 Governance and Management Objectives).

La gestión en cambio tiene que ver con planificar, construir, ejecutar y monitorizar las actividades para conseguir los objetivos estratégicos, en este sentido para COBIT responder de manera oportuna y efectiva a los problemas de TI requiere de una

mesa bien diseñada y desde luego de un proceso de gestión de incidentes que responda al escalamiento de incidentes, análisis de las ocurrencias, su causa raíz y su resolución; esto repercutirá en el aumento de la productividad y desde luego en generar confianza al usuario.

Gráfico 3, COBIT, Objetivos, Medición, Objetivos de Control - 2019 Governance and Management Objectives

3.1.3 NIST

La NIST es una institución norteamericana que se encarga de diseñar estándares y guías para las tecnologías y el sector industrial, por ende hay que entender que existen una serie de guías orientadas a cubrir diversos aspectos en el ámbito industrial – empresarial y de las tecnologías, una de ellas es la serie 800-61 Guía para la gestión de incidentes de ciberseguridad, en muchos casos como el de las tecnologías de información, NIST es bastante específica creando una serie de guías para cada uno de los elementos y entornos en los que puede estar envuelto la tecnología.

La guía 800-61 se encuentra estructurada en 3 aspectos importantes: planes de respuesta, gestión de incidentes y coordinación.

3.1.3.1 Planes de respuesta.

En este ámbito esta guía requiere el diseño de políticas y planes de respuesta frente a los incidentes y plantea la necesidad de contar con una estructura para responder

a los incidentes y la conformación de los equipos de respuesta (NIST SP 800-61r2) y en este sentido recomienda lo siguiente:

- Establecer un plan de respuesta formal ante incidentes, de cara a poder responder de manera rápida y eficaz cuando se vulneran las ciberdefensas.
- Diseñar una política de respuesta a incidentes, que defina qué eventos se consideran incidentes y cuáles son las funciones y responsabilidad de cada equipo y persona.
- Desarrollar un plan de respuesta que cuente con una hoja de ruta clara para ser implementado con éxito. Debe incluir objetivos y métricas para ser evaluado.
- Desarrollar procedimientos de respuesta a incidentes, con pasos detallados y que cubran toda la fase del proceso.
- Políticas y planes de respuesta frente a incidentes y estructura, personal y servicios de los equipos de respuesta.
- Estipular los procedimientos de intercambio de información relacionada con los incidentes. Desde medios, hasta autoridades.
- A la hora de establecer el modelo de equipo de respuesta hay que tener en cuenta todas las ventajas y desventajas, así como los recursos y necesidades de la organización.
- Es imprescindible seleccionar a los profesionales de estos equipos valorando sus habilidades, conocimientos técnicos, capacidad de comunicación y de pensamiento crítico. Prestarles formación es, también, fundamental.
- Identificar otros grupos dentro de la organización que deban participar en la gestión de los incidentes. Como, por ejemplo, un equipo de apoyo jurídico o el personal de gestión.
- Determinar el catálogo de servicios que debe ofrecer el equipo más allá de la respuesta a incidentes. Como la supervisión de los sistemas de detección de intrusiones de los que hablamos en el capítulo anterior. O la formación de todo el personal en lo que respecta a la ciberseguridad

3.1.3.2 Gestión De Incidentes.

Según NIST SP 800-61r2 - Handling an Incident, se establecen cuatro fases para la gestión de incidentes: preparación, detección y análisis, contención, erradicación y recuperación y actividades post incidente. Estas fases son cíclicas ya que lo que se busca es robustecer la respuesta para gestionar incidentes.

Para esto, NIST establece lo siguiente:

- Contar con herramientas y software útiles para la gestión de incidentes.
- Evaluar de manera recurrente los riesgos, de cara a prevenirlos.
- Identificar indicios de incidentes gracias al uso de varios sistemas de seguridad.
- Establecer mecanismos para que actores externos informen a la organización sobre incidentes.
- Imponer un nivel base de auditoría de todos los sistemas. Reforzándolo en los sistemas críticos.
- Perfilar redes y sistemas, lo que facilita la detección de cambios en los patrones y con ellos los incidentes.
- Conocer los comportamientos normales de las redes, los sistemas y las apps, de cara a detectar con facilidad cualquier otro tipo de comportamiento anormal.
- Crear una política de registro de la información sobre los incidentes. Comenzar a registrar todos los datos desde que exista la sospecha de que se ha producido uno. Y salvaguardarlos, puesto que incluyen información sensible sobre vulnerabilidades, fallos de seguridad y usuarios.
- Correlacionar eventos empleando diversas fuentes para obtener toda la información posible. En este sentido es importante mantener sincronizada la hora de los hosts.
- Emplear una base de conocimientos de información, fiable y consistente.
- Establecer un mecanismo para priorizar la gestión de los incidentes, basándose en factores clave como el impacto en el funcionamiento de la organización o la probabilidad de recuperación.
- Establecer estrategias de contención de los incidentes de manera rápida y eficaz.

3.1.3.3 Coordinación y compartición de la información.

Esta fase hace énfasis en la conformación y coordinación de equipos multidisciplinarios para atender un incidente y desde luego en los métodos y técnicas que se pueden emplear para atender un incidente (NIST SP 800-61r2 - Handling an Incident). Para esto el NIST recomienda.

- Planificar previamente la coordinación de los incidentes con los actores externos, como otros equipos de respuesta ante incidentes, autoridades o proveedores de servicios. De esta manera cada actor conocerá su función y la comunicación será mucho más eficiente.
- Contar con el asesoramiento permanente del equipo legal, para garantizar que todas las acciones de coordinación se ejecutan cumpliendo con el marco normativo.

- Intercambiar información sobre los incidentes a lo largo de todo su ciclo de vida. Desde la preparación hasta la actividad post-incidente.
- Automatizar el intercambio de información, en la medida de lo posible, de cara a que sea más eficaz y consuma menos recursos humanos.
- Analizar con precisión las ventajas e inconvenientes de compartir información sensible con otros actores.
- Compartir la mayor cantidad de información posible con otras organizaciones, teniendo en cuenta, siempre, los intereses de la organización y las razones de seguridad.

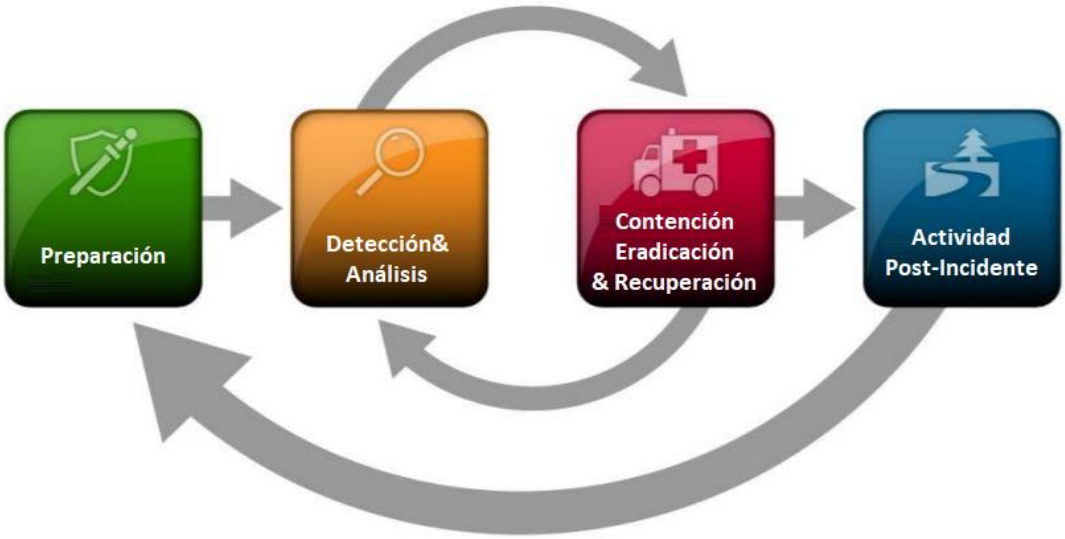


Gráfico 4, NIST SP 800-61r2 – Ciclo de Vida de la Respuesta a Incidentes.

3.1.4 ISO 27035

El estándar ISO 27001 para la Seguridad de la Información es una de las normas más utilizadas a nivel mundial, concretamente en Latinoamérica es uno de los importantes estándares para la seguridad de la información; de hecho, por citar tres ejemplos en países como: Perú, Colombia y Ecuador, han adoptado las ISO como si se tratara de una norma propia y las denominan norma técnica y el nombre de cada país, así en Ecuador el INEN la denomina NTE INEN-ISO/IEC 27001:2011. (**N**orma **T**écnica **E**cuatoriana).

La ISO 27035 aborda los 10 requisitos que los estándares ISO exigen; es decir, que este estándar puede ser aplicado independiente de la 27001 teniendo en cuenta que esta norma no es certificable; sin embargo, es recomendable que se implemente primero la 27001 y luego buscar el acoplamiento que sin duda se dará por ser de la misma familia.

Otro aspecto relevante de la ISO 27035 es que fundamente su gestión en el análisis de riesgos al igual que la ISO 27001, también plantea un esquema para la gestión de incidentes y establece la conformación de lo que se denomina ISIRT (Information Security Incident Response Team por sus siglas en inglés) o el Equipo de Respuesta a incidentes de Seguridad de información (CSIRT por sus siglas en inglés) que como todas las normas ISO plantea su funcionamiento en un ciclo de mejora continua, que se resume en 5 pasos:

Gráfico 5, ISO 27035, Etapas de la Gestión de Incidentes.

3.2 Comparativa de estándares y marcos

Como se ha comentado en líneas anteriores alrededor del mundo existen una serie de estándares y mejores prácticas que abordan de una u otra forma la necesidad de gestionar los incidentes, de ahí la importancia de analizar cada una de ellas al menos las más relevantes o adecuadas incluso por normativa o regulación del sector, para ello como se ha planteado se han tomado estándares y mejores prácticas de general aceptación sobre todo en Ecuador y que además también han sido tomadas en cuenta por los órganos de regulación especialmente del sector financiero cooperativo como la Superintendencia de Economía Popular y Solidaria (SEPS).

Gráfico 6, Cuadro comparativo de Marcos de trabajo, Estándares y guías.

Para el caso de ITIL y COBIT y de acuerdo a la breve descripción de este trabajo se puede decir que a pesar de su evolución para adoptar los retos de la empresa moderna en realidad lo que hacen respecto de los incidentes es abordarlos desde un enfoque del soporte que se brinda al usuario especialmente interno y en realidad no abordan de forma directa y tampoco proponen métodos que permitan atender los incidentes desde un enfoque de riesgos y continuidad del servicio, lo que los hace insuficientes para lo que pretende la Cooperativa Jardín Azuayo.

En el Caso de NIST 800-61 e ISO 27035 proveen herramientas para la gestión de los incidentes de seguridad de la información e incluso se puede decir que se complementan y robustecen; así por ejemplo mientras ISO indica el QUÉ, el NIST indica el CÓMO y eso hace que estas norma y guía sean seleccionadas para un diseño adecuado y acorde a las necesidades de la Cooperativa Jardín Azuayo.

3.3 CIBERSEGURIDAD.

No se puede hablar de incidentes de seguridad de la información sin antes no identificar el origen de estos eventos e incidentes de seguridad que pueden derivar fruto de las operaciones de una empresa o industria; para esto hay que reconocer que en el contexto de los servicios que una empresa puede ofertar se encuentra sí o sí envuelta la tecnología y como no puede ser de otra manera esta tecnología es

gestionada y usada por personas; así mismo, muchos de los servicios que las empresas ofertan se encuentran en línea; es decir, en el denominado ciberespacio [2], tal como lo hemos venido reconociendo este medio es demasiado hostil ya que aquí se encuentran cierto grupo de personas denominadas hackers [2], aunque lo correcto sería llamarlos crackers [2], no es motivo de este trabajo entrar a estas definiciones sino, reconocer que en el mundo del internet existen una serie de amenazas y una de ellas son los delincuentes informáticos que están al acecho para aprovechar las vulnerabilidades que la tecnología trae como propio de su naturaleza; a eso sumado que esta es operada, gestionada y administrada por personas y tal como se ha identificado por muchos expertos dentro de lo que se define como la cadena de la seguridad, el eslabón más débil es el factor humano, al fin la tecnología persé cumple un determinado propósito o función y su despliegue, operación, configuración, monitoreo, etc., está en manos de los responsables de dicha tecnología, a esto hay que agregar que esta es compleja y diversa, sumado a esto que además es costosa; entonces se trata de un entorno complejo al que hay que administrar eficiente y efectivamente con un presupuesto normalmente limitado; entonces se trata de una serie de factores a los que hay que gestionar de la mejor manera, es ahí que cobra sentido los estándares y frameworks donde se vinculan activamente a la alta gerencia con un rol preponderante para la gestión de las Tecnologías de la Información y Comunicación (TIC); sin embargo, es solo una parte de ella, porque como se ha mencionado esta tecnología aunque se trate de la mejor y la más actual está siempre propensa a fallos y vulnerabilidades y para esto abordar los aspectos de seguridad de la información, seguridad informática y ciberseguridad es crucial; por ello la adopción de estos estándares redundarán en brindar mayor solidez y confianza a las instituciones, por ende al usuario o cliente que se vale de los servicios que las empresa ofrecen.

Siendo que los servicios de una institución se encuentran expuestos en el internet con la finalidad de acercar los servicios y facilitar su acceso y disponibilidad 24/7, hay que dotarle de los elementos de protección adecuados y monitorizar constantemente para prevenir cualquier fallo o vulnerabilidad, es ahí cuando la gestión de incidentes cobra sentido, porque normalmente las operaciones

tecnológicas generar cientos o miles de registros (logs) por segundo y muchos de estos registros pueden corresponderse a datos de ataques, infecciones de malware o indisponibilidad de los servicios.

En resumen, la ciberseguridad hace referencia a todos los elementos y dispositivos que se encuentran conectados al internet tomando en cuenta que de lado y lado del internet existen usuarios que requieren de servicios y otros dispuestos a aprovechar las vulnerabilidades de la tecnología para enriquecerse ilegalmente, ya que hoy en día se reconoce al cibercrimen como el mayor generador de riqueza ilegal antes que el narcotráfico como lo citan en [3], ([4] y [5]:

3.4 Norma para el sector Cooperativo.

Desde el año 2013 el sector de la economía popular y solidaria cuenta con un órgano de control especializado para este sector, a partir de este año emitió un serie de resoluciones orientadas a atender diferentes ámbitos como la gestión financiera, gestión de riesgos, gobernanza, entre otros; a finales de 2017 emitió la Resolución 103 [6] denominada Seguridad en el Uso de Transferencias Electrónicas que busca "**Establecer los niveles mínimos de protección en las transferencias electrónicas realizadas mediante mensajes o instrucciones telefónicas**, electrónicas o celulares desde un ordenador conectado a redes de comunicación propias o de terceros a otro ordenador, mediante el uso de cualquier terminal". [tomado textualmente del sitio oficial de la SEPS]. En mayo de 2022 este órgano de control expidió la Resolución No. **SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002. NORMA DE CONTROL RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN EN LAS ENTIDADES DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO BAJO CONTROL DE LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA** [7], que "Regula los niveles mínimos para la administración de seguridad de la información que las entidades, la CONAFIPS[1] y las empresas, deben definir e implementar con el fin de resguardar y

[1] CONAFIPS. Corporación Nacional de Finanzas Populares y Solidarias

proteger sus activos de información, preservando su confidencialidad, integridad, disponibilidad y privacidad", en dicha norma consta una serie de artículos que hablan sobre la responsabilidad del Oficial de Seguridad de la Información (OSI) y en ciertos artículos se exige la implementación de procedimientos para la Gestión de Incidentes de Seguridad de la Información:

4. Oficial de Seguridad de la Información:

Entre sus responsabilidades, tendrá las siguientes:

a) Desarrollar, gestionar y monitorear el Plan Estratégico de Seguridad de la Información y el SGSI;
b) Diseñar y proponer las políticas, procesos, procedimientos, roles y responsabilidades para la gestión de seguridad de la información y del SGSI, al Consejo de Administración;
c) Solicitar la asignación de los recursos humanos, técnicos y financieros necesarios para la gestión de seguridad de la información, y velar que los mismos sean utilizados de forma eficiente y eficaz, alineados con los objetivos estratégicos institucionales;
d) Elaborar, implementar, mantener y actualizar las políticas, procesos, procedimientos, metodologías, planes y controles concernientes a la gestión de seguridad de la información, del SGSI, su mejora continua; y, una vez aprobados, difundirlos al personal que corresponde;
e) Desarrollar y ejecutar los Planes de Concienciación y Formación a su personal, en temas concernientes a seguridad de la información;
f) Coordinar y supervisar, con los responsables de los procesos del negocio, la implementación efectiva de los controles de seguridad de la información, establecidos en el plan de gestión de riesgos;
g) Desarrollar, coordinar, ejecutar, evaluar, proponer y comunicar el Plan de Gestión de Riesgos de Seguridad de la Información;
h) Coordinar las actividades para la gestión de seguridad de la información y del SGSI, incluyendo su implementación y seguimiento;
i) Definir, ejecutar y mantener procedimientos para la gestión de incidentes de seguridad de la información;
j) Velar que los involucrados internos y/o externos cuenten con los conocimientos y capacitación necesaria para el cumplimiento de sus roles y responsabilidades para la ejecución de procedimientos de respuesta ante incidentes;
k) Ejecutar los procedimientos y lineamientos establecidos, cuando se identifiquen incidentes de seguridad de la información;
l) Informar, de acuerdo con la normativa pertinente, los incidentes de seguridad de la información catalogados como sensibles o críticos, a las instituciones públicas que correspondan;
m) Participar en la evaluación de las amenazas de seguridad de la información y proponer medidas de mitigación;
n) Asesorar en materia de seguridad de la información, a través de su participación en los proyectos que involucren el manejo de información sensible o crítica de la misma, de sus socios, clientes y usuarios;
o) Recomendar medidas correctivas adicionales en temas relacionados de seguridad de la información, alineadas al Anexo 1, Régimen General y/o alineadas a buenas prácticas;
p) Verificar que los servicios prestados por personas naturales o jurídicas cumplan con las políticas de seguridad de la información establecidas; y,
q) Generar la documentación que evidencie la gestión de la seguridad de la información y del SGSI.

Gráfico 7, Responsabilidades del Oficial de Seguridad de la Información. Art. 12, numeral 4 Responsabilidades para la Seguridad de la Información.

Como se puede observar en la captura de la resolución 2022-002 de la SEPS, existen artículos específicos que solicitan que las instituciones traten y gestionen los incidentes de seguridad de la información y como la misma norma lo sugiere es necesario el apego o alineamiento a la serie del estándar ISO 2700X, por ello se busca construir una solución efectiva y eficiente para la Cooperativa Jardín Azuayo, que se ajuste a sus necesidades, pero sobre todo al contexto en el que se desenvuelve y no solo permita dar cumplimiento a lo exigido en la norma; sino, que se constituya en una herramienta para la Gestión de Incidentes y esto permita que los involucrados sepan cuál es su rol y función dentro de este ámbito y se pueda responder adecuada y oportunamente a los incidentes que se pueden suceder.

La gestión de incidentes debe permitir a quienes conformen el equipo saber cuándo y en qué momento se ha pasado de un evento a un incidente, cuando es necesario activar procedimientos de comunicación internos y cuando por su impacto en los servicios externos es necesario comunicar a los socios, clientes, usuarios e incluso órgano de control; así también, cuando es necesario activar el plan de continuidad del negocio y por último, el Plan de Recuperación de Desastres; es decir, este documento debe brindar toda la información para que se pueda responder a las siguientes interrogantes:

- ¿A qué se denomina incidente?
- ¿Cuándo un evento se convierte en un incidente?
- ¿Es necesario contar con un SOC?
- ¿Es necesario la conformación de un equipo multidisciplinario?
- ¿Quién o quiénes pueden reportar incidentes?
- ¿Quién es la voz oficial para comunicar un incidente y a quién?
- ¿Si el “incidente” afecta a procesos internos es necesario informar?
- ¿Es necesario un comité de crisis?

Al dar respuesta a estas interrogantes entonces se podrán establecer los aspectos en los que hay que trabajar para plantear un estudio aceptable y acorde a las necesidades institucionales:

- ✓ Procedimientos.
- ✓ Comunicación e información.
- ✓ Conformación del Comité de crisis.
- ✓ Conformación del equipo multidisciplinario.
- ✓ Activación de medidas de mitigación.
    - Activación del BCP.
    - Activación del DRP.
- ✓ Contacto con las autoridades.
- ✓ Retorno a la normalidad.
- ✓ Lecciones aprendidas.

3.4.1 Interrogantes a responder.

¿Cuándo un evento se convierte en un incidente?

Para responder esta pregunta y evitar ambigüedades en este estudio se toma textualmente las definiciones que el estándar ISO/IEC27000 indica al respecto; así mismo, es pertinente aclarar que es un evento de seguridad de la información, ya que esto permitirá una mejor claridad en este estudio y dará paso para una mejor comprensión de quienes integren el denominado equipo de gestión de incidentes de seguridad de la información (ISIRT, por sus siglas en inglés), pero más allá de esto, al tener claros estos conceptos se podrá definir procesos y procedimientos acordes a lo que pueda suceder; así mismo, permitirá establecer roles y funciones de quienes integren el equipo de gestión de incidentes.

Evento de Seguridad de la Información. Según el estándar ISO/IEC 27000:2009, indica: "Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad".

Incidente de Seguridad de la Información. Según el estándar ISO-IEC 2700:2009, indica: "Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información".

¿Cuándo un evento se convierte en un incidente?

De acuerdo con las definiciones antes mencionadas, entonces cuando un evento tenga una potencial probabilidad de comprometer la seguridad de los servicios institucionales: JA WEB (Página web transaccional), JA PAGOS (Aplicación para pago en tiendas, comercios, etc.), JA MOVIL (Aplicación móvil para acceder a servicios similares a los de la página web transaccional), ATMs (Cajeros Automáticos – Automatic Teller Machine), Sistema de informático de CORE y su disponibilidad se vea comprometida, entonces un proceso de gestión de incidentes debe entrar en funcionamiento.

Así mismo, si se ve comprometida la red de datos institucional entonces se dará paso al proceso de gestión de incidentes; para esto es necesario que los servicios sean monitoreados de forma constante 24/7/365, de ahí la necesidad de contar o conformar con SOC (Security Operation Center por sus siglas en inglés), este centro de monitoreo de operaciones de seguridad debe distinguir estos eventos y alertar o tomar procedimiento si el evento no pasa de ser solo una alerta que se lo puede gestionar sin mayores contratiempos.

¿Es necesario contar con un SOC?

De acuerdo a lo comentado, el monitoreo de los recursos tecnológico es fundamental y comprendiendo que a nivel tecnológico los eventos se miden en milisegundos entonces es necesario contar con equipamiento tecnológico y personal capacitado operando 24/7/365 (24 horas del día, los 7 días de la semana, todo el año), esto permitirá anticiparse si es posible y contrarrestar los posibles ataques o eventos que puedan acontecer y alertar al área de tecnología para posibles acciones y sobre todo al equipo de gestión de incidentes para su oportuna intervención.

¿Es necesario la conformación de un equipo multidisciplinario?

Sin duda es necesario que la Cooperativa Jardín Azuayo conforme un equipo para gestión de incidentes de seguridad de la información, mismo que debe ser capacitado en la investigación forense, análisis de datos, entre otros y con un conocimiento amplio en herramientas y soluciones apropiadas para atender los incidentes de manera oportuna y adecuada. Este equipo debe provenir de diferentes áreas de la cooperativa, sobre todo de tecnología; es decir, no puede ser un equipo externo; si no, personal que incluso conoce los procesos internos y puede entender la magnitud del problema; así mismo, se debe identificar con claridad los proveedores críticos y soporte externo en caso de ser necesario su ayuda o contribución y estos deben ser debidamente informados para su intervención de ser necesario; para ello será necesario incluir en los contratos cláusulas que permita contar con dicho apoyo.

¿Quién o quiénes pueden reportar incidentes?

Siendo que las operaciones de una entidad financiera como la Cooperativa Jardín Azuayo soporta sus operaciones en la tecnología casi en su totalidad y entendiendo que existen diferentes actores en el ecosistema institucional se debe comprender que los eventos se pueden reportar desde diferentes áreas, personas (colaboradores, directivos, usuarios) de los sistemas de información de la cooperativa y desde luego que las herramientas de seguridad desplegadas puedan reportar a manera de alertas y que deberían ser parte del ámbito de monitoreo del SOC, aquí la clave es determinar un proceso adecuado y contar con un solo punto de entrada que consolide dichas alertas y las comunique, en este sentido la mesa de ayuda es fundamental; para esto se plantea el siguiente esquema de operación:

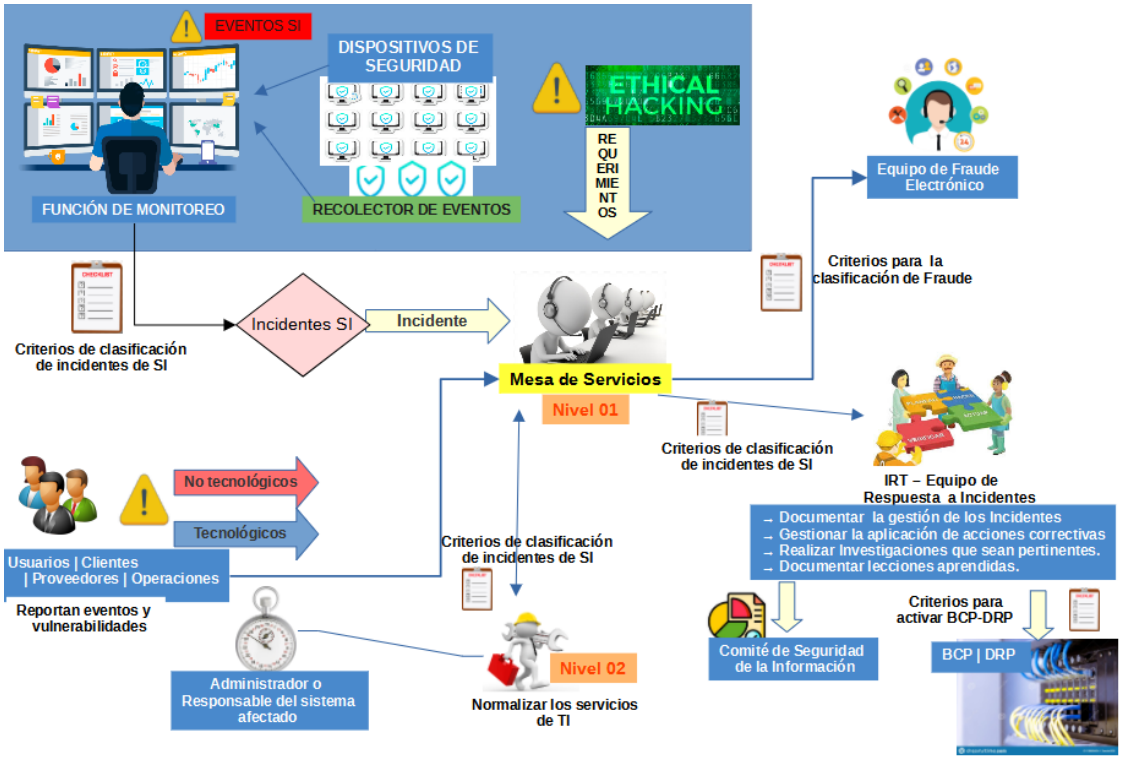


Gráfico 8, Esquema propuesto de atención única a los eventos e incidentes de seguridad

Como se observa en el esquema propuesto para la atención, se puede notar que los incidentes pueden venir desde diferentes instancias, como el centro de monitoreo de seguridad, un socio, proveedor, empleado, etc.; sin embargo, quien consolida estos requerimientos es la denominada Mesa de Ayuda, a continuación se analiza y se da la característica de incidente, esto se logrará a partir de tener una adecuada capacitación, luego deriva al equipo de respuesta a incidentes quien toma la investigación y alternativas de solución; todo esto bajo la supervisión del Oficial de Seguridad de la Información; para de ser necesario; es decir de acuerdo al impacto convocar al Comité de incidentes y de ser necesario activar el plan de recuperación de desastres.

¿Quién es la voz oficial para comunicar un incidente y a quién?

Se debe dejar claro que cuando un incidente ha sucedido y ha comprometido la disponibilidad de los servicios institucionales, se está teniendo una serie de reclamos a nivel de los socios, clientes y usuarios y cada uno con diferentes posibilidades de externalizar su malestar o queja; en este sentido las redes sociales juegan un papel crucial, pues que no se responda adecuada y oportunamente, pero sobre todo de forma

oficial pueda causar daños en primer lugar reputacionales graves y luego incluso derivar en sanciones o multas de los órganos de control; sin mencionar la posible afectación o desconfianza que los socios puedan tener, incluso pudiendo afectar seriamente su estabilidad institucional; para ello es necesario identificar una persona que maneje las redes sociales, esta persona debe ser objetiva y sobre todo mantenerse en constante comunicación interna con el comité de crisis para saber la forma a adecuada de informar; su perfil debe ser analizado cautelosamente, ya que un amplio y acertado criterio para dar respuesta a las más diversas quejas, reclamos e insultos puede determinar que la "llama" se extienda o tergiverse; por otra parte es necesario un profesional en comunicación social que pueda orientar a la alta dirección y al gerente para llevar un mensaje sereno, claro y preciso sobre lo que puede estar ocurriendo; por último, la persona llamada a responder ante un incidente que ha comprometido la disponibilidad de los servicios es el gerente general.

Ningún funcionario a parte de los referidos en líneas anteriores, podrán dar una respuesta oficial o formal sin antes la autorización del gerente y de la aprobación del mensaje oficial. Desde luego el ente de control será el primero en ser comunicado porque en determinado momento ayudará a mantener la calma.

¿Si el "incidente" afecta a procesos internos es necesario informar?

Sí, porque un evento que comprometa sistemas de información que no necesariamente afecte algún servicio externo, debe ser reportado internamente para el conocimiento de la alta gerencia, ya que, cada área es proveedor y cliente de las otras, entonces cuando un servicio interno es afectado sin duda afecta a otra área impactando en sus funciones o tareas y esto a su vez pueden en algún momento derivar en algo más complicado como la afectación de un servicio externo; de ahí la necesidad de comunicar internamente.

¿Es necesario un comité de crisis?

Cuando un incidente tiene una afectación interna no es necesario conformar un comité, más, si es necesario informar; sin embargo, cuando un incidente afecta la disponibilidad de los servicios institucionales externos, es necesario conformar el denominado comité de crisis, de aquí se desprenderá el mensaje a difundir tanto a medios de comunicación, como en redes sociales y sobre todo quien lo debe hacer. Así también, aquí se podrá

obtener los posibles recursos o acciones que se puedan requerir para solventar el incidente. Quienes integraran este comité en primer lugar por el Gerente General, Gerente de Innovación y Desarrollo (antes área de TI), Gerente de Servicios, Director de Finanzas y Oficial de Seguridad de la Información; en caso de ser necesario se podrá convocar a otras personas de interés.

Al responder estas interrogantes se pretende enfocar las acciones y/o actividades fundamentales que se deben ejecutar para que la Gestión de Incidentes de Seguridad de esta manera será una herramienta para la Cooperativa Jardín Azuayo. Con estos insumos entonces plantearemos las acciones necesarias para que este estudio brinde las acciones necesarias para la gestión de incidentes en el siguiente capítulo

4. Propuesta de Implementación del sistema de Gestión de Incidentes

En el capítulo anterior se plantearon unas interrogantes y sus respuestas deben ser base para plantear una propuesta de implementación del sistema de gestión de incidentes de seguridad de la información para la Cooperativa Jardín Azuayo que responda al requerimiento regulatorio, pero sobre todo a la necesidad que por su giro del negocio y del servicio se requieren.

4.1 Proceso para la Gestión de Incidentes.

No se puede pretender proponer un estudio para la implementación del sistema de gestión de seguridad de la información sin antes no plantear de manera estructurada la forma de como atender un incidente, determinar el camino exacto por donde debe fluir la solución e identificar la o las personas claves que pueden aportar a la solución, así mismo, comprendiendo que el origen de un incidente puede ser diverso, como diversos sus efectos, es necesario diseñar un proceso que permita ser eficiente y efectivo al momento de resolver un incidente, para esto es necesario conocer la institución, observar su forma de trabajo, conocer su estructura organizativa y funcional; así como, conocer los servicios, productos o soluciones que ofrece para a partir de esto dimensionar el campo de acción y determinar un flujo adecuado de atención.

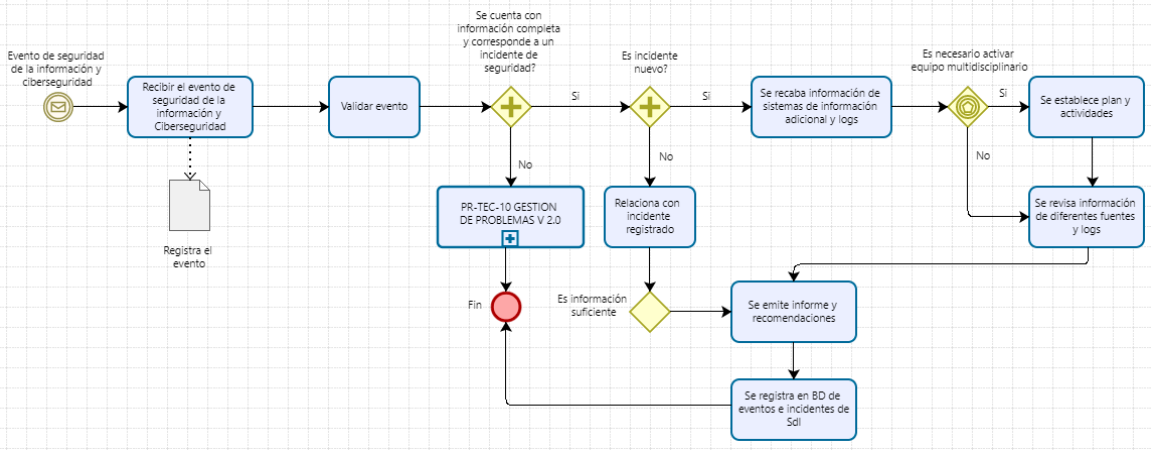


Gráfico 9, Proceso de Gestión de Incidentes propuesto.

Un evento de seguridad puede venir desde diferentes instancias: socios, colaboradores, usuarios, proveedores, etc., y puede tener diferentes categorías, como, por ejemplo:

- Un usuario interno que indica que al descargar un documento su equipo se apagó.
- Un socio que indica que la página web transaccional simplemente no está disponible.
- El equipo de seguridad perimetral (Firewall) reporta demasiadas peticiones a los servicios, lo que hace que colapsen.
- Un colaborador ha incumplido la política de seguridad de la información.

Como se puede observar existen diferentes causas u orígenes para un incidente, pero lo correcto es decir evento, ya que solo la investigación y el grado de repercusión sobre los servicios determinará la magnitud del evento y si se lo trata como incidente de allí la necesidad de identificar con claridad un incidente y determinar su impacto o criticidad, para ello es necesario tener en cuenta la gestión de riesgos y la clasificación de los incidentes:

Gestión de Riesgos de Seguridad de la Información.

Para una eficaz gestión de incidentes de seguridad de la información es necesario tomar en consideración los activos de información y colocar su objetivo en aquellos que hayan

sido identificados como altos y críticos, para esto debe apoyarse en la metodología de gestión de riesgo de seguridad la información que se encuentra descrita en el Manual de Seguridad de la Información vigente (MA-AYC-01 Manual-SDI.pdf); así también se debe tener en cuenta los siguientes aspectos:

Vulnerabilidades. Es necesario la revisión frecuente de las vulnerabilidades a las que están expuestas la tecnología sea esta de hardware o software y su nivel de criticidad, así también es necesario contar con un inventario detallado de los activos de información tecnológica donde se encuentre descrito los servicios que soporta cada una de ellas, esto permitirá tener un enfoque práctico y adecuado para la gestión de vulnerabilidades.

Clasificar los tipos de incidentes. Siendo que los incidentes de seguridad de la información pueden ser causadas por acciones humanas deliberadas o accidentales y también por medios técnicos. Es necesario establecer una categoría que permita identificar y clasificar los incidentes de seguridad de la información, así como determinar si se trata de un evento o incidente; para ello se deben tener en cuenta las siguientes categorías que ISO/IEC 27035 ha definido:

Categoría	Descripción	Ejemplos
Incidente de desastre natural	Causada por desastres naturales que están por fuera del control humano.	Terremotos, volcanes, inundaciones, ciclones, rayos, tsunamis, derrumbes,
Incidente de disturbios sociales	Causada por inestabilidad de la sociedad.	Ataque terrorista, guerra, manifestaciones, etc.
Incidente de daño físico	Causada por acciones físicas accidentales o deliberadas.	Incendio, agua, electrostática, ambiente nefasto (contaminación, polvo, corrosión congelamiento), destrucción, robo, pérdida, alteración de equipos, medios, etc.
Incidente de fallas de infraestructura	Causada por fallas en los sistemas y servicios básicos que apoyan el funcionamiento de los sistemas de información	Fallas en la alimentación eléctrica, en las comunicaciones, aire acondicionado, en el suministro de agua, etc.
Incidente de perturbación por radiaciones	Causada Por perturbaciones debidas a radiaciones	Radiación electromagnética, pulsos electromagnéticos, interferencia electrónica, fluctuación de tensión, radiación térmica, etc.
Incidentes de falla técnica	Causada por fallas en los sistemas de información o en instalaciones no técnicas relacionadas; al igual que problemas humanos no intencionales que dan como resultado la no disponibilidad o destrucción de los sistemas de información.	Falla del hardware, mal funcionamiento del software, sobrecarga (saturación de la capacidad de los sistemas de información), violación de la mantenibilidad, etc.
Incidente de malware	Causada por programas maliciosos creados y divulgados en forma deliberada. Un programa malicioso se inserta en los sistemas de información para afectar la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones o sistemas	Virus, gusanos, troyanos, botnets, backdoors, rasomware, etc.

	operativos, y/o afectar la operación normal de los sistemas de información.	
Incidente de ataque técnico	Causada por el ataque a sistemas de información, a través de redes u otros medios técnicos, ya sea mediante el aprovechamiento de la vulnerabilidad de los sistemas de información en cuanto a configuraciones, protocolos o programas, o por la fuerza, lo que da como resultado un estado anormal de los sistemas de información, o daño potencial a las operaciones presentes del sistema.	Escaneo de redes, aprovechamiento de vulnerabilidades, puertas traseras, intentos de ingreso, interferencia, denegación de servicios, etc.
Incidente de violación de reglas	Causada por violación de las reglas en forma accidental o deliberada.	Uso no autorizado de recursos, violaciones de los derechos de autor, etc.
Incidente de compromiso de las funciones	Causada al poner en riesgo en forma accidental o deliberada las funciones de los sistemas de información en cuanto a seguridad.	Abuso de derechos, falsificación de derechos, denegación de acciones, operaciones equivocadas, violación de la disponibilidad del personal, etc.
Incidente de puesta en riesgo de la información	Causada al poner en riesgo en forma accidental o deliberada la seguridad de la información (CID)	Interceptación, espionaje, divulgación, enmascaramiento, ingeniería social, phishing, smishing, vishing, robo de datos, pérdida de datos, alteración de datos, errores de datos, análisis de flujo de datos, detección de posición, etc.
Incidente relacionado con contenidos peligrosos	Causada por la propagación de contenido indeseable a través de redes de información	Contenido ilegal, contenido que provocan pánico, contenido malicioso, contenido abusivo, etc.

Otros incidentes	No clasificados en ninguna de las categorías de incidentes anteriores.	

Gráfico 10, Categorías de incidentes de seguridad de la información, de acuerdo con las amenazas. Tomado de la Norma ISO / IEC 27032.

4.2 Comunicación e Información.

En el entorno financiero donde se desenvuelve la cooperativa Jardín Azuayo y donde siempre estará bajo el escrutinio público, así como de los órganos de control, ofrecer información adecuada y oportuna en caso de un incidente puede significar la permanencia de la cooperativa en el mercado, conservar a sus socios o, todo lo contrario; llevar un mensaje claro, sereno y sobre todo que venga de los representantes de la cooperativa servirá para dar la tranquilidad a los socios, clientes y usuarios, una comunicación asertiva permitirá dar tranquilidad y que mejor que el gerente general sea el llamado a realizar esa comunicación.

Desde luego no es lo mismo un incidente donde el core financiero no esté disponible, que uno donde solo estén indispuestos los ATMs (Cajeros automáticos), de ahí la necesidad de establecer escenarios:

Escenario 1. Caída de servicios de atención directa en oficina (operaciones de ahorro y crédito) por una hora.

Comunicación. Mensaje entregado por los colaboradores que están en contacto directo a los socios; si se extiende por más tiempo comunicado oficial por sus canales formales y por parte del área de comunicaciones. Si la interrupción supera las 4h comunicado formal por parte del gerente general y a través de medios de difusión formales.

Escenario 2. Caída de servicios virtuales (Página web transaccional) entre una y cuatro horas.

Comunicación. Mensaje publicado en la página web informativa, redes sociales y servicios de call center y operaciones. Si la interrupción supera las 4h

comunicado formal por parte del gerente general y a través de medios de difusión formales.

Escenario 3. Caída de todos los servicios, tanto físicos como electrónicos. Por dos horas o más.

Comunicación. Comunicado oficial del gerente de la cooperativa a la SEPS, y comunicado en conjunto. Se analizará necesidad de rueda de prensa.

4.3 Conformación del Comité de Crisis.

El nivel o criticidad del incidente determinará la necesidad de conformar un comité de crisis; sin embargo, es necesario tener previsto su integración, los miembros que deberían de manera fija conformar dicho comité son: Gerente General, Gerente de Servicio, Gerente de Tecnología, Asesor Legal, Director de Seguridad de la Información y Director de Comunicaciones; quedará a discreción y de acuerdo al incidente la necesidad de incorporar otras personas como puede ser el Gerente de Talento Humano.

4.4 Conformación del Equipo de Respuesta a Incidentes.

Como se ha podido establecer, un incidente puede tener diferentes orígenes e impactos, así también puede tener diferentes implicaciones, por lo tanto se debe conformar un equipo multidisciplinario que desde el punto de vista de su experiencia y capacidad puedan contribuir a solventar el o los incidentes que puedan suceder; conociendo que más del 95% de las actividades de la cooperativa se desarrollan a través de la tecnología, siempre se debe contar con el apoyo de personal de dicha área de la misma manera conociendo que la tecnología es amplia, como amplia las especialidades se deberá contar con personal experto en desarrollo, redes informáticas, infraestructura; así como personal de operaciones y estos a su vez dirigidos por el director de seguridad de la información.

Así mismo, queda abierta la posibilidad de involucrar al equipo a personal experto de otras áreas que de acuerdo con el incidente podrá contribuir, de la misma manera se podría analizar la necesidad de contar con personal externo como pueden ser proveedores estratégicos o personas expertas que puedan asesorar.

4.5 Activación de medidas de mitigación.

Un usuario que recibe un correo con un adjunto y descarga, luego el equipo se reinicia debe ser aislado de la red; un servicio virtual que no está disponible requiere un poco más de investigación, porque puede deberse a una actualización que no ha sido probada y por consiguiente colapsó el servicio o puede ser por un ataque de denegación de servicios. Saber reaccionar es clave, de ahí la necesidad de contar con planes de contingencia que permitan una transición entre la normalidad y el caos.

Gráfico 11, Etapas de la Transición de Incidentes.

La gestión de incidentes de seguridad de la información es una forma de prever y anticiparse a cualquier situación disruptiva que vulnere estas garantías, para ello debemos estar preparados y organizados para atender las alertas que los controles pueden mostrar.

Es importante que la gestión de incidentes sea parte y se integre con los procesos de la cooperativa junto con la estructura general del sistema de gestión de seguridad de la información.

Cada vez son más frecuentes y cercanos los ataques a las infraestructuras críticas y sus servicios, el sector que más afección tiene es sin duda el sector financiero en el que se desenvuelve la cooperativa, por ello, el monitoreo de los controles establecidos, así como la atención que se dé a las alarmas o alertas de seguridad es primordial y necesario.

La Cooperativa debe estar prepara para realizar una transición de acuerdo con la situación, es decir, basada en estados donde se pueda establecer la operación normal y de acuerdo con el monitoreo de las alertas se pueda reconocer eventos críticos y dar atención a un posible compromiso de los servicios institucionales.

Gráfico 12, Descripción de las Etapas de la Transición de Incidentes.

Contar con Planes de Continuidad del Negocio (BCP), así como con un Plan de Recuperación de Desastres Informáticos (DRP) es una necesidad para la cooperativa a parte que por aspectos regulatorio los debe tener; así, estos planes normalmente han sabido considerar escenarios enmarcados en los desastres naturales; sin embargo, dado la realidad actual, esto resulta intrascendente, más cuando se observa como alrededor del mundo e incluso en nuestro país instituciones aparentemente fuertes y robustas tecnológicamente hablando han sufrido ataques que les ha representado miles e incluso millones de dólares en pérdidas; en este sentido tomar en cuenta dentro del DRP sobre todo, escenarios como la denegación de servicios, un ataque por malware ,etc., es de vital importancia y necesidad. En este sentido la gestión de incidentes debe determinar en qué momento se debe activar el DRP.

4.6 Contacto con las Autoridades.

Cuando un incidente trasciende las fronteras internas de las operaciones institucionales y afecta a los socios en el desarrollo de sus transacciones tanto de captaciones (Ahorro) y de colocaciones (crédito) tanto de manera física como virtual y además toma demasiado tiempo en recuperar la normalidad de las operaciones; cuando el Plan de Recuperación de Desastres no está cumpliendo su cometido, es necesario informar a las autoridades de control a fin de comunicar lo que está sucediendo; ya que en determinado momento es el órgano de control (Superintendencia de Economía Popular y Solidaria - SEPS) que se vuelve garante de las instituciones, que operan dentro del marco de la ley; desde luego junto al órgano de control deberán estar los representantes de la cooperativa como son el Gerente General y el Presidente del Consejo de Administración.

4.7 Retorno a la Normalidad.

Hay que definir que es la normalidad, servicios arriba y operativos, recursos al 100%, pueden ser tomados con indicios de normalidad; sin embargo, corroborar o comprobar que los servicios virtuales se encuentran operativos y funcionales; así como, los servicios de atención presencial se han restablecido se considera “normalidad”.

Pero ¿cómo fue este retorno?, ¿cuáles fueron los daños colaterales?, ¿cuáles los daños directos?, ¿cuáles son los daños o la afectación a la imagen? y ¿cuánto dañó en lo legal? ¿Qué procesos internos y externos se han activado; por ejemplo, la auditoría interna y/o externa por parte de órgano de control están en ejecución?, son preguntas a las habría que responder con la mayor justeza y la verdad, asumiendo siempre que no ha existido dolo o intención detrás de un fallo, entendiendo que la mayor afectación sin duda estará en la parte reputacional y desde luego legal; más aún con regulaciones y normativas vigentes donde ya se exigen la implementación, pruebas y ejecución de los planes de continuidad y de recuperación de desastres.

En este contexto, la normalidad puede ser visto desde tres puntos de vista:

1. Servicios activos y operativos disponibles 24/7;

2. Impacto o afectación reputacional, donde dependiendo como se a manejado el o los incidentes el impacto puede ser fuerte, llevando a la deserción de socios (desvinculación), retiro de capitales, etc., y

3. la afectación legal donde las sanciones o multas impuestas por los órganos de control serán establecidas en torno al análisis de incumplimiento normativo que se establezca.

De estos 3 aspectos, sin duda el más importante es el reputacional, porque la pérdida de confianza no solo de socios propios, sino, del mercado nacional sin duda determinará la estabilidad financiera y la continuidad de la institución en el sector financiero nacional de ahí la importancia de desarrollar planes de recuperación acordes al contexto.

Todo esto desde el punto de vista del restablecimiento de los servicios; es decir, desde lo operativo; pero, determinar que fue lo que realmente pasó, como se dio tal o cuál incidente, por donde se originó la brecha, que recursos fueron comprometidos, cuáles son las huellas o pistas que pueden ayudar a determinar y responder estas interrogantes; de ahí la necesidad de contar con dos insumos necesarios:

- Pistas y Logs de auditoría.
- Informes del Monitoreo del SOC (Security Operation Center).

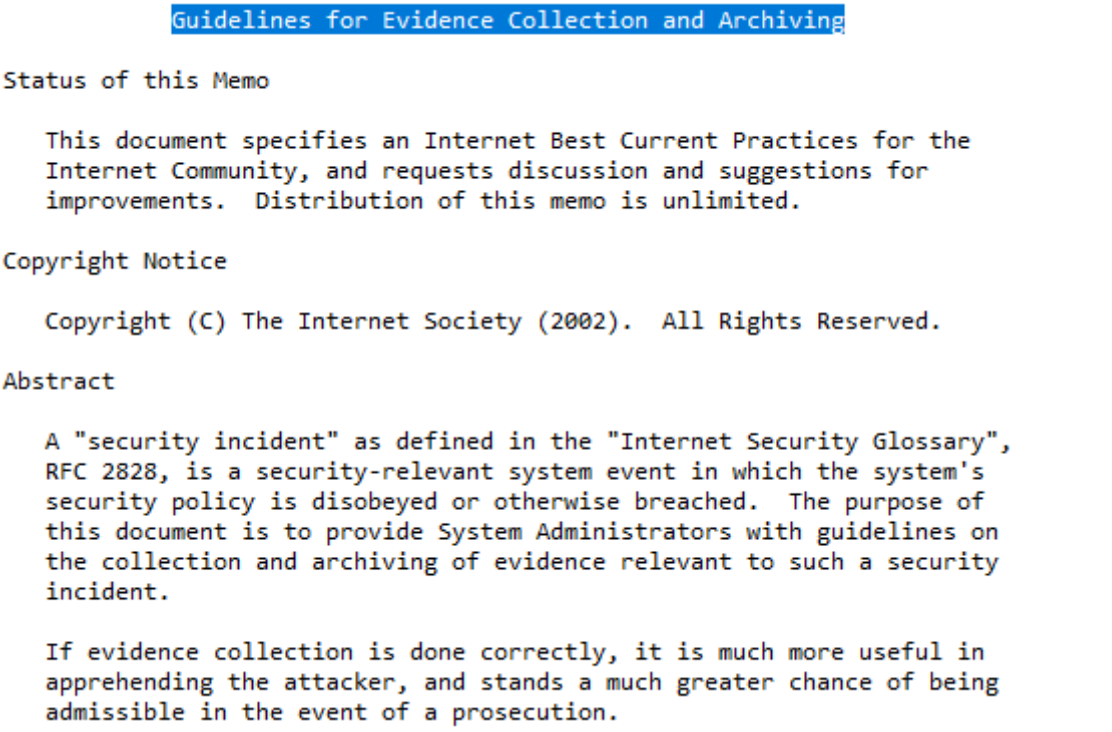
Pistas y Logs de Auditoría: Es importante diferencia entre una pista de auditoría y un log.

Un **Log** es un registro que se activa en un sistema de información; es decir, dentro de un sistema operativo o sistema de información solo basta activarlo para obtener el log de un determinado suceso; por ejemplo, en sistemas Windows, un log se consigue activando dentro del visor de eventos el log o características de las que se requiere tener el seguimiento.

En cambio, la **Pista** de auditoría son registros que los desarrolladores programan dentro de los sistemas de información para obtener datos o registros de las operaciones que se han ejecutado, ejemplo: en un sistema financiero se pueden programar pistas de auditoría para obtener la fecha, hora, nombre de la aplicación, nombre del sistema operativo origen y destino de una transacción, es decir, se desarrolla a conveniencia y necesidad; en cualquier caso estas pistas y logs servirán para dar trazabilidad a los eventos que puedan suceder en las infraestructuras y servicios tecnológicos.

De acuerdo con lo descrito se vuelve imprescindible contar pistas y logs de auditoría, ya que serán uno de los insumos indispensables al momento de realizar la investigación, dar trazabilidad a los eventos e identificar si es posible el origen y causa del incidente.

Aplicar técnicas de investigación forense es necesario ya que esto permitirá racionalizar la evidencia obtenida; pero, sobre todo la forma de obtener la evidencia y su preservación adecuada permitirá o brindará la capacidad de demostrar lo sucedido repitiendo los hechos incluso podrá ayudar a emprender acciones legales sustentadas y fuertes en caso de una defensa legal; para esto se sugiere aplicar el RFC 3227 (Rquest For Comments) Guidelines for Evidence Collection and Archiving.



Guidelines for Evidence Collection and Archiving

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

A "security incident" as defined in the "Internet Security Glossary", RFC 2828, is a security-relevant system event in which the system's security policy is disobeyed or otherwise breached. The purpose of this document is to provide System Administrators with guidelines on the collection and archiving of evidence relevant to such a security incident.

If evidence collection is done correctly, it is much more useful in apprehending the attacker, and stands a much greater chance of being admissible in the event of a prosecution.

Gráfico 13, Directrices para la recopilación y el archivo de pruebas

Existen muchos estándares para recolección de evidencia; sin embargo, el RFC 3227 para recolección de evidencia digital es de amplio uso y de las más recomendad a nivel mundial, “para que descubrir el agua tibia”.

4.8 Lecciones Aprendidas.

Llevar un registro de todos los incidentes, sus causas, efectos, acciones realizadas para identificar, tipos de investigación que se realizaron e incluso el tipo de perfil o cargos de personal especializado que ayudó a resolver un incidente, es básico para poder establecer estrategias de prevención y evitar que vuelva a suceder.

Las lecciones aprendidas deben derivar en una serie de acciones encaminadas a evitar que vuelva a suceder un incidente, que si sucede su impacto sea el mínimo, así como la afectación a los servicios. Involucrar a la plana gerencial es fundamental.

Por último, estas lecciones deben ayudar a concienciar al usuario, pero sobre todo a la plana gerencial y directiva, ya que, a partir de su comprensión se podrá solicitar recursos para evitar o por lo menos contrarrestar los efectos de un incidente.

5. Resultados y discusión

De acuerdo con este estudio, más que importante es necesario que la cooperativa Jardín Azuayo implemente un sistema de gestión de incidentes, más allá de la exigencia regulatoria del ente de control (SEPS), ya que el sistema permitirá trabajar en la prevención y ese es el principal objetivo del sistema; un adecuado monitoreo tanto interno como externo, deben por lo menos disminuir o reducir el impacto de un evento adverso. Hay que reconocer que jamás el riesgo en el contexto en el que se desenvuelve la cooperativa va a desaparecer; sin embargo, ayudará a establecer medidas, controles y planes de acción que permitirán atender un incidente de acuerdo con su magnitud e impacto, así como, a través de contar con un proceso determinará los pasos para atender un determinado incidente y saber con quienes se puede contar para estos casos y activar a las instancias adecuadas a fin de responder ágil y efectivamente.

En toda organización y en Jardín Azuayo no es la excepción siempre preocupa que las erogaciones de dinero no sean un gasto sino una inversión y si esa inversión apoya objetivos estratégicos entonces recibirá el apoyo mayoritario de un grupo gerencial; en este sentido se plantea un análisis de retorno de la inversión (ROI por sus siglas en inglés) que demostrará que el sistema de gestión de incidentes debe ser prioridad en su planificación operativa (POA).

Como es sabido el ROI "**permite evaluar la rentabilidad de una inversión en base al capital destinado y al beneficio obtenido**" de esta manera las empresas esperan observar el valor de retorno de determinada inversión; sin embargo, este no es el caso de una inversión orientada a la seguridad, ya que lo que la cooperativa va a recibir no es ingreso de dinero; por ejemplo, cuanto es el retorno de inversión por la implementación de un software antimalware o por la compra de un WAF (Web Application Software por sus siglas en inglés), la respuesta es cero retorno; en este sentido las inversiones en seguridad no son para obtener rentabilidad al menos no de la manera que tradicionalmente se plantea; sin embargo, esto no quiere decir

que no se deba medir o peor aún que no se pueda; lo que sucede es que el análisis estará orientado por cuanto es la proyección que se busca reducir o contrarrestar respecto de un incidente o cuál es el impacto económico que se evitará; así mismo, cuanto es lo que se puede evitar si la base de datos institucional se daña o deja de operar, cuanto pierde la cooperativa, esa información se puede obtener a partir de conocer cuantas transacciones se procesan por minuto, por todas las sucursales y cuanto es el promedio de las mismas. Por otra parte, contar con un registro de los incidentes es ideal; a este tipo de análisis se denomina ROSI (Return on Security Investment – Retorno de inversión en seguridad). Por lo general, las áreas de presupuestarias o financieras siempre preguntan cuál es el retorno o ganancia que se planea obtener; pero cuando se habla de seguridad en realidad la pregunta es **¿cuánto dinero perdería la cooperativa por determinado incidente?**

Para responder esta pregunta, antes se debería responder estas otras:

¿Cuál es la probabilidad que ocurra un incidente?

¿Cuál es el costo de la(s) medida(s) de prevención?

¿Cuánto tiempo es el retraso de las operaciones?

¿Cuánto es la pérdida aproximada que se puede tener?

Pueden existir otras muchas preguntas, que dependiendo el grado de minuciosidad o detalle se puedan formular, sin embargo, estas preguntas podrían considerarse como base para el análisis, en este sentido la fórmula del ROSI es:

ROSI = *((No. Incidentes x costo incidente) – inversión) / Inversión x 100 (para obtener en porcentaje)*.

Como se puede observar es muy sencillo calcular el costo de inversión para prevenir incidentes de seguridad; lo que hay que tomar en cuenta es que lo factores de riesgo y pérdida de la cooperativa dependen de muchos factores, por lo que tener estos

valores al alcance no es sencillo, de ahí la necesidad de documentar y registrar los eventos e incidentes de seguridad con el mayor detalle posible.

5.1 Retorno de Inversión en Seguridad (ROSI)

Para proyectar adecuadamente el ROSI se analiza el contexto en el que el sector financiero se desenvuelve y donde es más notorio un ataque de malware que cifra la base de datos principal o de CORE, el análisis sería de la siguiente manera.

Solución de backup es una inversión de $ 120.000 anual.

La facturación anual de Jardín Azuayo es $ 164.000.000,00 / 365 días = $ 449.315,07 diario / 24 horas = $ 18.721,46 hora.

Un incidente de Rasomware puede dejar a la cooperativa 3 días sin servicios ($ 1.347.945,21).

Los ciberdelincuentes, solicitan un rescate de 100 bitcoins x $ 27.873,00[2] = $ 2.700.000,00.

La generación de respaldos en línea puede minimizar el riesgo y mantener la disponibilidad del servicio sin pagar el rescate.

ROSI = ((No. Incidentes x costo incidente) – inversión) / Inversión x 100 (para obtener en porcentaje)

ROSI = ((1 x $ 1.347.945,21) - $ 120.000) / $ 120.000,00 x 100

ROSI = 1.023% de justificación del proyecto.

[2] Valor referencial tomado el 25 de marzo de 2023 del sitio: https://www.google.com/finance/quote/BTC-usd

Cuando a los supuestos se dan valores que, si bien son aproximados, pero con un gran ajuste de la realidad, será fácil justificar una inversión de este estilo, lo que indica que trabajar en prevención siempre será ventajoso y rentable; de aquí que es totalmente justificable trabajar en prevención de incidentes.

6. Conclusiones

Alrededor del mundo existen una serie de estándares, marcos de trabajo y mejores prácticas que ya incorporan aspectos relacionados con la gestión de incidentes, alinear estos estándares para implementar un sistema de gestión que se ajuste a las necesidades de la cooperativa es lo adecuado.

En el país los órganos de control del sector financiero como la Super Intendencia de Bancos (SB) y la Superintendencia de Economía Popular y Solidaria (SEPS) han incorporado una serie de regulaciones para robustecer la Seguridad de la Información y la gestión de incidentes, esto sin duda permitirá que las instituciones del sector financiero potencialicen sus procesos y trabajen en prevención; anticiparse es mejor que llegar.

Trabajar en prevención es fundamental; ya que el impacto de un incidente puede ser devastador y a lo mejor no exista retorno. Para esto es crucial apoyarse en la gestión de riesgos y visibilizar el impacto en caso de evento.

Siendo siempre importante que las inversiones reflejen un beneficio para la cooperativa; es necesario que se visualice adecuadamente que las inversiones de seguridad tienen su beneficio no por el retorno sino por el ahorro o prevención de que se materialice un incidente.

Contar con sistema de gestión de incidentes integral donde se tome en cuenta los activos de información críticos (servicios, infraestructura, personas, etc.) y que este sea parte del sistema de gestión de seguridad de la información permitirá proactividad y resiliencia

Referencias

GUIA TECNICA COLOMBIANA GTC-ISO/IEC 27035. (2012-12-12). Tecnología de la información, TECNICAS DE SEGURIDAD. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Bogota.

COBIT 2019. (2018). ISACA. USA

NIST. (2012). Computer Security Incident Handling Guide (Revisión 2.). US

ITIL. (2019). Information Technology Infrastruture Library. AXELOS (Version 4). UK

[1] https://www.cci-es.org/consecuencias-de-los-ataques-a-la-ciberseguridad-en-infraestructuras-criticas/, «https://www.cci-es.org,» 11 08 2022. [En línea]. Available: https://www.cci-es.org/consecuencias-de-los-ataques-a-la-ciberseguridad-en-infraestructuras-criticas/.

[2] rfc1983, «datatracker.ietf.org/doc/rfc1983/,» 08 1996. [En línea]. Available: https://datatracker.ietf.org/doc/rfc1983/.

[3] R. El Universo, «www.eluniverso.com/larevista/tecnologia,» 19 04 2022. [En línea]. Available: https://www.eluniverso.com/larevista/tecnologia/el-aumento-de-la-ciberdelincuencia-a-escala-de-economia-mundial-nota/.

[4] L. República, «https://www.larepublica.co/empresas,» 30 09 2022. [En línea]. Available: https://www.larepublica.co/empresas/el-costo-global-del-cibercrimen-en-2025-ascendera-a-un-total-de-us-10-5-billones-3458183.

[5] D. Occidente, «https://occidente.co,» 15 12 2022. [En línea]. Available: https://occidente.co/secciones/tecnologia/cuanto-costo-el-cibercrimen-en-2022/.

[6] SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103, «www.seps.gob.ec,» 23 11 2017. [En línea]. Available: https://www.seps.gob.ec/wp-content/uploads/Resolucion-No.-SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103.pdf.

[7] SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002, «www.seps.gob.ec,» 03 05 2022. [En línea]. Available: https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf.

[8] J. Calles-García y P. González-Pérez, La Biblia del Footprinting, 2011.

[9] www.elhacker.net, «www.elhacker.net,» [En línea]. Available: https://www.elhacker.net/trucos_google.html.

[10] I. E. d. Normalización, «TECNOLOGÍAS DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) - REQUISITOS,» de *Norma Técnica Ecuatoriana NTE-INEN-ISO/IEC 27001:2011*, Quito, 2011.

[11] G. Westreicher, 1 09 2020. [En línea]. Available: https://economipedia.com/definiciones/retorno-de-la-inversion-roi.html.