Universidad Tecnológica del Chocó
Diego Luis Córdoba

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Gestión Informática

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ Cra. 22 No 18B-10

TABLA DE CONTENIDO

INTRODUCCIÓN

Una política de gestión de incidentes de seguridad de la información es un componente crucial para establecer una postura de seguridad sólida dentro de una organización.

La seguridad de la información es de vital importancia para la Universidad Tecnológica del Chocó. Reconocemos que los incidentes de seguridad son una realidad en el entorno actual de amenazas cada vez más sofisticadas y persistentes. Por lo tanto, es fundamental que tengamos una respuesta efectiva y coordinada ante estos incidentes para minimizar el impacto y proteger nuestros activos de información críticos.

Esta Política de Gestión de Incidentes de Seguridad de la Información establece los principios, objetivos y responsabilidades para la detección, respuesta, mitigación y recuperación de incidentes de seguridad de la información en nuestra organización, Esta se aplica a todos los empleados, contratistas, socios comerciales y terceros que manejan o tienen acceso a nuestra información confidencial.

Universidad Tecnológica del Chocó Diego Luis Córdoba
Nit. 891680089-4
Carrera 22 No. 18B-10 B. Nicolás Medrano – Ciudadela Universitaria
Conmutador (+57) 4 6726565, Línea gratuita: 018000 938824
E-mail: contactenos@utch.edu.co, Página Web: utch.edu.co
Quibdó, Chocó (Colombia)

I.- DEFINICIONES ESTRATÉGICAS

La Universidad Tecnológica del Choco, a través de su Comité de Riesgos y Seguridad de la Información, en adelante el Comité de Incidentes de Seguridad de la Información, presenta en este documento la Política de Gestión de Incidentes de Seguridad, que aborda los procedimientos orientados a la mitigación y corrección de vulnerabilidades y amenazas que pudieran afectar la seguridad de la información institucional y/o la continuidad operacional de los servicios que presta la universidad.

a.- Objetivos específicos

- Establecer responsabilidades de las distintas Unidades en relación con la seguridad de los datos de la empresa (integridad, disponibilidad y confidencialidad), ya sea se encuentren en la plataforma informática como en su manipulación a cargo de los funcionarios en general.
- Responder en forma rápida, eficaz y ordenada ante la ocurrencia de incidentes de seguridad que afecten los activos de información de la empresa.
- Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

b.- Alcance

Esta política se aplica a todos los trabajadores y terceras partes que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información de la Universidad Tecnológica del Chocó. También se aplica a cualesquiera de sus relaciones con terceros que impliquen el acceso a sus datos,

utilización de sus recursos o a la administración y control de sus sistemas de información.

Esta política rige independientemente del lugar en el trabajador presta sus servicios a la organización, total o parcialmente, e indistintamente de la modalidad de trabajo ya sea “presencial”, “a distancia”, “teletrabajo” u otra, en las condiciones que establezca la legislación vigente, los planteamientos de la Dirección del Trabajo o los Estados de Excepción Constitucional decretados por el presidente de la República.

Esta política gobierna la seguridad de la información de todos los procesos estratégicos de la Universidad Tecnológica del Choco, establecidos en sus estatutos que la rigen y en general por lo establecido en el Ministerio de las Tic específicamente en el marco de Gobierno Digital, cubriendo a toda la organización independiente de su ubicación geográfica en el país.

Marco legal

- DECRETO 1078 DE 2015 Decreto Único Reglamentario del sector TIC. En particular las normas atinentes a la Estrategia de Gobierno en Línea.
- Ley 1273 de 2009, Por medio de esta Ley se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos", y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1712 de 2014 (Uso de las TIC) Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información.
- NTC/ISO 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. NTC/ISO 27002 Estándar para la seguridad de la información
- NTC/ISO 27032 Estándar de Ciberseguridad

- Resolución 1519 de 2020, Anexo 3 Condiciones Mínimas técnicas y de Seguridad Digital

c.- Roles y Responsabilidades

Las responsabilidades se encuentran definidas en la política de la organización de la seguridad de la información.

d.- Vigencia y Actualización

La Política se considera vigente desde la fecha de su aprobación por parte de la autoridad, documento que será revisado y actualizado cada año o cuando el Comité de Riesgos y Seguridad de la Información lo determine, o toda vez que se produzca un cambio significativo que modifique el nivel de riesgo presente de la Universidad Tecnológica del Chocó.

La Política deberá ser revisada por el Comité de Seguridad de la Información. No obstante, aquello, la Unidad responsable de Ciberseguridad promoverá la revisión permanente de esta Política y generará las propuestas de actualización que sean necesarias, con el objetivo de apoyar el ciclo de mejora continua del SGSI.

Entre los cambios que hacen necesaria la revisión de las políticas, se debe destacar:

- Cambios en las leyes o reglamentos que afecten a la Universidad Tecnológica del Choco.
- Incorporación o modificaciones relevantes de procesos críticos de la Universidad Tecnológica del Choco.
- Cambios significativos al soporte tecnológico.

- Modificaciones en la estructura de la organización.
- Cambios significativos en los niveles de riesgo a que se expone la información.
- Cambios relevantes en las Definiciones Estratégicas.
- Ajustes necesarios producto de Estados de Excepción Constitucional.
- Ajustes necesarios para proteger las infraestructuras críticas.

Las revisiones que se efectúen a la Política de General de Seguridad de la Información deben considerar tanto la actualidad de ella, como su eficacia, eficiencia y cumplimiento.

e.- Revisión del cumplimiento

El Comité de Riesgos y Seguridad de la Información, anualmente, asignará la responsabilidad de ejecutar un proceso formal de revisión del cumplimiento a cargo de una o varias unidades organizacionales, pudiendo optar también por una revisión independiente interna o una externa ejecutada por una tercera parte.

Además, este Comité determinará la metodología y los alcances que estime necesarios para cumplir los objetivos estratégicos de revisión y cumplimiento de las políticas y su mejora continua.

f.- Control de documentos

Los documentos requeridos por el Sistema de Gestión de la Seguridad de la Información (SGSI) deben protegerse y controlarse. Con este objetivo, las acciones necesarias a implementar son:

Universidad Tecnológica del Chocó Diego Luis Córdoba
Nit. 891680089-4
Carrera 22 No. 18B-10 B. Nicolás Medrano – Ciudadela Universitaria
Conmutador (+57) 4 6726565, Línea gratuita: 018000 938824
E-mail: contactenos@utch.edu.co, Página Web: utch.edu.co
Quibdó, Chocó (Colombia)

- Revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.
- Registrar los cambios o actualizaciones de los documentos una vez que son aprobados por el Comité de Riesgos y Seguridad, incorporando Tabla en Capitulo final en cada documento.
- Se deberá controlar el uso no intencionado de documentos obsoletos.
- En caso de mantenerse los documentos por cualquier propósito, éstos deberán tener una adecuada identificación a efecto de diferenciarse de los vigentes.

Las versiones pertinentes de los documentos aplicables se encontrarán disponibles para quienes lo necesiten y serán almacenados y transferidos de acuerdo con los procedimientos aplicables a su clasificación.

g.- Difusión

El mecanismo de difusión de la Política será a través de la Intranet, circulares informativas, correos electrónicos masivos o cualquier otro medio que el Comité de Riesgos y Seguridad de la Información estime pertinente, procurando apoyar la sensibilización con infografías que faciliten la comprensión de esta por todos los usuarios en general.

II.- MODO DE OPERACIÓN

a.- Responsabilidades y procedimientos

La Oficina de Sistemas y Soporte Técnico, con el responsable de la Seguridad Digital de Se, adoptará un rol activo como responsable técnico de establecer procedimientos

ante el Comité, que permitan garantizar una respuesta rápida, eficaz y ordenada ante los incidentes de ciberseguridad relacionados con la plataforma tecnológica que administra la Oficina de sistemas y soporte Técnico. Por otra parte, las Unidades dueñas de los datos a que pertenecen los usuarios de los sistemas, son responsables del manejo que den a los datos institucionales, lo que deberá ser supervisado por las jefaturas correspondientes y colaborar con fortalecer una cultura de atención a las anomalías y su oportuna notificación.

b.- Unidades responsables respecto de los datos institucionales

Las siguientes Unidades deberán establecer directrices respecto a sus competencias en relación con la protección de los datos y garantizar la continuidad operativa de los servicios y productos de la empresa tanto internos como externos, con la debida difusión y control de cumplimiento a cargo de las respectivas jefaturas.

- *Oficina de Sistemas y Soporte Técnico*: En lo que se refiere a la plataforma tecnológica.
- Dispositivos de almacenamiento de los datos: En lo que se refiere al uso, manipulación y protección de acceso a datos de la empresa de modo de garantizar su integridad, disponibilidad y confidencialidad.

c.-Informe de las debilidades de la seguridad de la información

Se exigirá a todo el personal y contratistas que utilizan los sistemas y servicios de información de la Universidad Tecnológica del Chocó registrar e informar sobre cualquier debilidad o actividad sospechosa en cuanto a la seguridad de la información de los sistemas o servicios. Esta función es importante para la institución, pues en la medida que el personal está alerta a estos detalles se maximiza la vigilancia y resguardo de los activos institucionales.

En este sentido el personal deberá siempre estar alerta tanto a los temas de respeto a las políticas de seguridad de la información como a señales que parezcan extrañas o poco habituales, teniendo en consideración que cada uno de ellos puede ser blanco u objetivo de un ataque cibernético mediante el cual se puede acceder a información personal o de la empresa. Se destacan, entre otros, los siguientes:

- Credenciales o contraseñas.
- Direcciones de correo electrónico.
- Cargos y roles.
- Lógicas de los procesos internos (dependencias jerárquicas, procesos críticos como control de las cuentas corrientes de la empresa, entre otros)
- Teléfonos y redes sociales.
- Perfiles de usuario o gustos personales de compras y/o navegación web.
- Información confidencial (documentos sensibles institucionales, tarjetas de crédito, entre otros).
- Recursos del sistema (CPU, RAM y disco duro), para almacenar malware y/o utilizar equipos institucionales sin autorización.

d.- Procedimientos para gestión de Incidentes tecnológicos la planificación y preparación de la respuesta ante incidentes.

A continuación, se presentan los procedimientos que debe cumplir la Oficina de Sistemas y Soporte Técnico para cumplir con el resguardo de la plataforma y datos que le competen.

Planificación y preparación de la respuesta ante incidentes

La Oficina de Sistemas y Soporte Técnico deberá informar continuamente al Comité de Seguridad de la Información acerca del análisis de entorno de amenazas con el objetivo de planificar y preparar respuesta a incidentes en lo que a su componente de

prevención esté al alcance. Estos informes agregados mensualmente o cuando la severidad de las amenazas lo ameriten, serán reportados a la Dirección o Alta Gerencia.

El sistema de monitoreo y alertas deberá proveer estadísticas e informes de tendencia para apoyar el análisis de entorno.

Se deberá mantener actualizado Plan de contingencia generado a partir de la matriz de riesgos que pudieran afectar a la plataforma y a la seguridad de los datos de la empresa, levantada por cada Unidad y que son categorizados y priorizados por la Oficina de Sistemas y Soporte Técnico y aprobados por el Comité de Riesgos y Seguridad de la Información.

En relación con los riesgos informáticos, la Oficina de Sistemas y Soporte Técnico, preparará un Plan de monitoreo, identificación de principales contactos involucrados en los distintos ámbitos, ya sean internos o externos.

Procedimientos para monitorear, detectar, analizar e informar sobre eventos e incidentes de seguridad

Se mantendrá un servicio de monitoreo continuo para detectar analizar e informar sobre eventos e incidentes de seguridad, lo que estará a cargo de la Oficina de Sistemas y Soporte Técnico, a través de herramientas tecnológicas, servicios de terceros, y recursos humanos internos. Cada herramienta de monitoreo debe dejar registro de los servicios monitoreados y de los eventos detectados.

Será obligatorio tener un sistema de monitoreo principal (Plan A) y uno o más sistemas de monitoreo alternativos (Plan B y Plan C) como contingencia en caso de falla del plan A. Para los planes B y C se deberán utilizar formas innovadoras y eficientes desde el punto de vista técnico y económico, pudiendo estar basadas en tecnología propietaria,

tecnología de código abierto (OpenSource) o desarrollos propios, pero deberá tener la suficiente fortaleza para diferenciarse de la plataforma del Plan A y no verse afectada por sus vulnerabilidades o fallas.

Procedimientos para registrar actividades de administración de incidentes

Cada evento o incidente de relevancia se consignará en el sistema de tickets dispuesto como herramienta central de registro y gestión de los incidentes, con objetivo central de notificar y disponer de un registro central de los incidentes. De esta última plataforma se podrán extraer estadísticas de gestión de incidentes y hacer análisis que aporten datos al proceso de mejoramiento continuo.

En la herramienta centralizada de reporte y notificación de incidentes quedarán registradas también las actividades de administración de los incidentes para procesos de evaluación o generación de aprendizaje ante errores y/o aciertos.

Procedimientos para administrar evidencia forense

En general los aspectos forenses estarán acotados a la relevancia del incidente y a facultades administrativas pertinentes para el caso en estudio, y resguardando los principios de la política general.

La institución contará con registros logs de las principales aplicaciones y/o dispositivos de control de manera que sin acceder en primera instancia a los activos de información de los usuarios se podrá tener señales indirectas de actividades anómalas.

Cuando el incidente tenga caracteres de delito y se haya judicializado su investigación, se deberán dar las facilidades respectivas al organismo policial competente para que acceda y rescate toda la evidencia necesaria, acorde a las facultades legales que un juez o fiscal hayan entregado e instruido.

Universidad Tecnológica del Chocó Diego Luis Córdoba
Nit. 891680089-4
Carrera 22 No. 18B-10 B. Nicolás Medrano – Ciudadela Universitaria
Conmutador (+57) 4 6726565, Línea gratuita: 018000 938824
E-mail: contactenos@utch.edu.co, Página Web: utch.edu.co
Quibdó, Chocó (Colombia)

Como medida general la empresa procurará en la medida de lo posible y según la evolución de madurez del programa de ciberseguridad instalar las buenas prácticas que hay en el mercado y organismos internacionales sobre la materia, pudiendo al menos considerar el estándar ISO 27037.

e.- Procedimientos para la evaluación y la decisión sobre los eventos de seguridad de la información

La empresa establecerá a través de su organización interna, la debida priorización de los activos de información de manera que las instancias técnicas tengan las directrices necesarias para establecer un análisis de riesgo acorde a las amenazas y el riesgo potencial.

La evaluación de los incidentes deberá contar con insumos como las definiciones estratégicas y de negocio de la empresa, la prioridad de los procesos, y un análisis de riesgos basado en lo posible en algunas normas internacionales, tales como ISO 27005 o ISO 31000 entre otros.

La evaluación de las debilidades en la seguridad de la información es un proceso reflexivo que se llevará adelante utilizando herramientas tecnológicas y de análisis de especialistas, tendientes a producir informes que permitan apoyar la toma de decisión.

El modelo mínimo para considerar es el que dice relación con la Matriz Probabilidad-Impacto que permite priorizar las tareas de una forma visual y sencilla, basándose en las dos dimensiones esenciales relativas al riesgo:

- La probabilidad de que el evento suceda.
- El impacto que provocaría en caso de que sucediese.

f.- Gestión de Incidentes

La institución llevará adelante la respuesta a incidentes a través de sus instancias técnicas y se coordinará con el Comité de Riesgos y Seguridad de la Información en la medida que el impacto de los incidentes afecte a los procesos críticos de la institución.

Cabe destacar que en la medida que los incidentes hayan sido judicializados, se requerirán de especiales cuidados, en orden a convocar a los expertos policiales para que accedan a la información necesaria para la investigación.

Los problemas relacionados a los incidentes de seguridad de la información dentro de la organización serán manejados por el Encargado de Ciberseguridad, el que se apoyará con el personal de la Oficina de Sistemas y Soporte Técnico y la Oficina Jurídica, con atención al resguardo de los principios de la Política General y las leyes vigentes. A su vez, el Encargado de Ciberseguridad mantendrá los contactos correspondientes con las autoridades, grupos de interés externos o foros que manejen los problemas relacionados con los incidentes de seguridad de la información.

Notificación de un Incidente de Seguridad

El personal o terceras partes deberán informar, tan pronto como sea posible, debilidades, eventos o incidentes que pueda tener un impacto en la seguridad de los activos de la organización. Esto no implica que están autorizados a iniciar proactivamente análisis de seguridad de sus entornos o aplicativos, pues mientras el whitehacking no se encuentre regulado en nuestra legislación, será considerado como una acción hostil y eventualmente como un delito informático.

Existen tres mecanismos de contacto para la notificación de un incidente de seguridad por parte de un usuario afectado:

- Correo electrónico: gestionderiesgos@utch.edu.co
- Notificación telefónica al número telefónico:

- A través del formulario electrónico del sitio web: https://www.utch.edu.co

Cabe destacar que eventualmente existirán incidentes que puedan tener un impacto mayor o significativo respecto de la afectación a datos confidenciales, internos, personales de clientes o generar una disrupción importante en el funcionamiento de la empresa. Para estos incidentes, además del procedimiento regular de notificación deberá considerarse la notificación a la entidad reguladora del sector según directivas sectoriales establecidas o al CSIRT de Gobierno por los medios electrónicos definidos para tales efectos.

Registro de un Incidente de Seguridad

El Encargado de CiberSeguridad al recibir la notificación, revisará que los antecedentes sean consistentes y completos con el objetivo de iniciar la evaluación del incidente y determinar su prioridad. Si faltan antecedentes, el Encargado de Seguridad debe solicitarlos al usuario afectado por el incidente o responsable del sistema involucrado, quien tendrá un plazo de un día hábil para entregar la información faltante (procurando que sea lo antes posibles atendiendo a las altas velocidades de propagación de los malware actuales).

Una vez que el Encargado de CiberSeguridad posea los antecedentes necesarios, registrará el incidente de seguridad en el Sistema de Gestión de Incidentes.

Recopilación de evidencia

La Institución establecerá procedimientos referenciales para la identificación, recopilación, adquisición y preservación de la información que pueda servir de evidencia.

Este esfuerzo estará relacionado con la magnitud del incidente y en ningún caso buscará competir con los procesos forenses policiales, en caso de ser catalogado como delito y se haya ejecutado la correspondiente judicialización de este.

Se pondrá especial foco en el resguardo de registros logs de las diferentes aplicaciones que resguardan la seguridad interna y/o proveen la operación de los principales servicios institucionales, buscando la menor afectación posible de la privacidad de los funcionarios.

En la medida que la necesidad de profundización de los procesos forenses sean claves para el resguardo de los activos de la información de la empresa los procedimientos deberán ajustarse a la normativa internacional ISO 27037 u otra que la reemplazare.

Análisis y Evaluación de un Incidente de Seguridad

El Encargado de CiberSeguridad analiza los antecedentes, clasifica el incidente y deriva requerimientos de información a las Áreas internas pertinentes o Proveedores externos TI u otros según corresponda, a fin de recolectar antecedentes.

Una vez que el Encargado de CiberSeguridad recibe la información sobre las causas del incidente, identifica alternativas de solución y, en caso de que la solución implique costos, debe cuantificarlos para colaborar con las gestiones relativas a su aprobación.

Asimismo, deberá registrarse en el Sistema de Gestión de Incidentes de Seguridad, la información recopilada, descripción, responsables, análisis de la ocurrencia del incidente, tiempo de respuesta y solución al incidente, finalmente cuantificar y monitorear el tipo, volumen y costo del incidente. En caso de que haya implicancias legales o de otro tipo, deberá poner los antecedentes en conocimiento del la alta gerencia y oficina Juridica para acordar un curso a seguir.

Como buena práctica se considerará, en lo posible, realizar las denuncias pertinentes al sistema judicial cuando se detecte la comisión de delitos informáticos y la notificación

oportuna a las personas afectadas (usuarios, personal o clientes) cuando estuvieren involucrados datos personales de éstos.

En el caso de incidentes que afectan la plataforma tecnológica de la empresa, se involucrará a la [unidad TIC], la cual aplicará los procedimientos de respuesta específicos que permiten de una manera ordenada, estandarizada, segura y eficaz responder las anomalías que afectan la seguridad de la información. Toda respuesta a eventos o incidentes significativos deberá al menos incluir los siguientes aspectos para un mejor desempeño y atención del incidente:

- Recopilar la evidencia lo más pronto posible después de la verificación, teniendo a la vista las buenas prácticas sobre estos procedimientos (ISO 27037), de manera de no afectar la evidencia y su cadena de custodia en una posible judicialización posterior.
- Realizar análisis forenses de seguridad de la información, según sea necesario.
- Escalamiento, según sea necesario.
- Asegurarse de que todas las actividades de respuesta se registren correctamente para el posterior análisis.
- Comunicación de la existencia del incidente de seguridad de la información o cualquier detalle pertinente a otras personas o unidades internas o externas que deban ser informadas o advertidas sobre estos incidentes.
- Manejar las debilidades de la seguridad de la información que causan o contribuyen al incidente.
- Una vez que se ha manejado el incidente correctamente, se deberá cerrar y registrar formalmente.

Dependiendo de la magnitud del impacto materializado para la institución, se realizará un análisis post-incidente, para identificar el origen de este, y en lo posible establecer una atribución que permita tomar decisiones jurídicas y estratégicas.

Universidad Tecnológica del Chocó Diego Luis Córdoba
Nit. 891680089-4
Carrera 22 No. 18B-10 B. Nicolás Medrano – Ciudadela Universitaria
Conmutador (+57) 4 6726565, Línea gratuita: 018000 938824
E-mail: contactenos@utch.edu.co, Página Web: utch.edu.co
Quibdó, Chocó (Colombia)

Monitoreo del estado y progreso de un Incidente de Seguridad

El Encargado de CiberSeguridad debe monitorear que los plazos acordados respecto al compromiso de resolución del incidente de seguridad sean cumplidos por parte del responsable de su ejecución. Además, debe mantener informado al usuario afectado/denunciante, acerca del progreso de la solución del incidente.

Revisará y evaluará que la mitigación aplicada cumple lo requerido.

Revisará y propondrá mejoras a los controles, procesos y procedimientos involucrados, que pudieren haber fallado en evitar la materialización de las amenazas específicas involucradas en el incidente gestionado.

Protección de evidencias de un Incidente de Seguridad

El [Encargado de CiberSeguridad] debe recolectar, retener y proteger las evidencias, en caso de que se deba seguir una acción legal contra la persona u organización responsable del incidente de seguridad de la información, dentro de lo posible con lineamientos normativos tales como ISO 27.037 u otro grupo de buenas prácticas que ayuden a preservar la evidencia digital y su cadena de custodia.

Cierre de un Incidente de Seguridad

El Encargado de CiberSeguridad, una vez que está seguro de que la solución al incidente fue implementada exitosamente, registra el cierre del incidente en la Planilla de Incidentes de Seguridad y envía respuesta al usuario afectado/denunciante, notificando del cierre del incidente.

La base de datos de incidentes que se genere al interior de la empresa será revisada con intervalos no mayores a un año para verificar que los mismos no se repitan o si se han modificado las circunstancias, desarrollar una nueva medida de control que

minimice la posibilidad e impacto del incidente en caso de que se diera la posibilidad de volver a presentarse.

Contenidos mínimos de los informes de procedimientos

Con el propósito de evitar la ocurrencia de incidentes que afecten la seguridad de la información institucional, se plantea la mantención de procedimientos que ayuden a recordar las actividades necesarias, en especial para los incidentes analizados y resueltos. Estos procedimientos deberán ser generados por las áreas involucradas y son parte de su resolución, lo que quedará registrado en el historial de este:

- Propuestas de formularios de informes de eventos de seguridad de la información para apoyar la acción del informe y ayudar a la persona que lo hace a recordar todas las actividades necesarias en caso de un evento de seguridad de la información;
- El procedimiento que se debería realizar en caso de un evento de seguridad de la información, es decir, indicando todos los detalles inmediatamente, como el tipo de incumplimiento, si ocurre una falla, los mensajes en la pantalla e informar inmediatamente al punto de contacto y realizar solo acciones coordinadas;
- Referencia a un proceso disciplinario formal establecido respecto del personal que caen en incumplimientos de seguridad.
- Procesos de retroalimentación adecuados para asegurarse de que a aquellas personas que informan eventos de seguridad se les notifique sobre los resultados una vez que se ha abordado el problema y se haya cerrado.

Universidad Tecnológica del Chocó Diego Luis Córdoba
Nit. 891680089-4
Carrera 22 No. 18B-10 B. Nicolás Medrano – Ciudadela Universitaria
Conmutador (+57) 4 6726565, Línea gratuita: 018000 938824
E-mail: contactenos@utch.edu.co, Página Web: utch.edu.co
Quibdó, Chocó (Colombia)

g.- Informe de eventos de seguridad de la información

Los eventos de seguridad de la información se informarán a través de los canales establecidos por el [Comité de Riesgos y Seguridad de la Información], siendo al menos los siguientes:

- Correo electrónico.
- Informe escrito autorizado por el Encargado Ciberseguridad.
- Comunicación telefónica y/o mensajería electrónica debidamente resguardada.
- Página web de intranet, en caso de que corresponda.
- Se debe contemplar más de un canal, pues es posible que el incidente afecte a uno de dichos medios de comunicación.
- Las situaciones que se han de considerar en el informe de eventos de seguridad incluyen, al menos, las siguientes:
- Identificación de control de seguridad ineficaz.
- Detección de incumplimiento de la integridad, la confidencialidad o las expectativas de disponibilidad de la información.
- Errores humanos.
- Incumplimientos con las políticas o pautas.
- Incumplimientos en las disposiciones de seguridad física.
- Cambios no controlados en el sistema.
- Fallas en el software o hardware.
- Violaciones de acceso.
- Situaciones tipificadas en la Ley colombiana.

Las fallas u otro comportamiento anómalo del sistema pueden ser un indicador de un ataque de seguridad o un incumplimiento real de seguridad y, por lo tanto, siempre se deberá informar como un evento de seguridad de la información.

Dependiendo de la magnitud para la institución se realizará un análisis post-incidente, para identificar el origen del incidente.

h.- Aprendizaje de los incidentes de seguridad de la información

Se realizarán informes de evaluación de los incidentes ocurridos de manera de poder concentrar el conocimiento obtenido de los diferentes análisis y la respectiva resolución y/o mitigación de los incidentes de seguridad de la información, para que este aprendizaje ayude a reducir la probabilidad o el impacto de incidentes futuros.

Estos informes serán ingresados como insumo al proceso de mejoramiento continuo de los controles, procesos, políticas y procedimientos de la empresa.

Proyectó	Elaboró	Revisó	Fecha	Folios
Jilmar Chaverra Barcos Profesional Especializado Líder Seguridad Digital	**Jilmar Chaverra Barcos** Profesional Especializado Líder Seguridad Digital	**Yunner Eduard Moreno Córdoba** Jefe de Sistemas y Soporte Técnico.	05-04-2023	22

Universidad Tecnológica del Chocó Diego Luis Córdoba
Nit. 891680089-4
Carrera 22 No. 18B-10 B. Nicolás Medrano – Ciudadela Universitaria
Conmutador (+57) 4 6726565, Línea gratuita: 018000 938824
E-mail: contactenos@utch.edu.co, Página Web: utch.edu.co
Quibdó, Chocó (Colombia)