Asignatura	Datos del alumno	Fecha
Delitos Informáticos	Apellidos: Paz López	06/02/2022
	Nombre: Angel Ramon	

INTRODUCCION

En la actualidad en el área de informática y medios de comunicación se hace eco de los avances que nos ha traído lo que es la tecnología en las diferentes áreas donde el ser humano se desenvuelve, ya sea por la alta gama de aparatos o dispositivos electrónicos que ayudan al ser humano a comunicarse, a realizar actividades, sistemas informáticos que ahorran tiempo al momento de realizar algún proceso entre otros, pero tras ello también se puede convertir en un arma de doble filo, ya que así como hay cosas positivas con el avance de la tecnología también podemos encontrar cosas negativas, como ser las conductas delictivas que han crecido con los avances tecnológicos, la cual ha abierto las puertas a delincuentes a poder realizar actividades de robo mediante el internet, ingresando a los sistemas para realizar fraudes, robo, destrucción de información y entre otras actividades que infringen la ley, es por ello es necesario que todas las empresas e instituciones que manejen tecnología y área de informática se atienda y regulen normas, políticas en cuanto al uso de las computadoras, sistemas informáticos. Para ello realizamos un documento o manual para detección de Delitos Informáticos con la finalidad de que las empresas tengan una adecuada Gestión de Seguridad de la Información cumpliendo con la preservación de la confidencialidad, integridad y disponibilidad de los activos de la organización tomando como base los lineamientos en la Norma la ISO IEC 27001.

OBJETIVO

Gestionar adecuadamente todos los incidentes y eventos negativos que pudieran ocasionar riesgos a los activos de la organización por ello se debe contar con procesos estructurados y contar con la planificación eficaz para reducir y manejar cualquier tipo de incidentes de seguridad en cuanto a la información.

ROLES Y RESPONSABILIDADES

- **Gerentes**

La Gerencia de la Seguridad de la organización es quien tiene toda la responsabilidad de la seguridad total de los activos de la organización involucrando las áreas de TI y la alta dirección en las actividades de seguridad, como ser planificación de todas las actividades y procesos de gestión de incidentes y eventos de seguridad. La gerencia y la alta dirección son los encargados de estipular las normas, políticas, procedimientos de seguridad y hacerlas llegar mediante capacitaciones a los empleados de la organización.

- **Empleados**

Los empleados deberán hacer el debido reporte de cualquier evento sospechoso que pudiese ocasionar algún daño a los activos de la organización de manera inmediata al gerente o al equipo de seguridad encargado. Es importante que los empleados conozcan las políticas y normas de seguridad de la organización y a la vez estos estén comprometidos con su trabajo y a los objetivos y metas de la organización.

- **Oficial de Seguridad de la información**

Es el responsable de orientar y realizar el tratamiento a todos los incidentes de seguridad que se reporten y realizar el seguimiento y monitoreo a los mismos, comunicar los procesos y actividades, planificación de respuesta a los incidentes, gestión de riesgos.

DETECCION DE INCIDENTES

Todos los empleados de la organización deben estar capacitados mediante campañas de sensibilización con respecto a la seguridad de la información y conocer los medios o formas que pueden ocasionar algún ataque o incidente en la seguridad que pueden afectar los objetivos y metas de la organización, como ser ataques que tengan que ver con:

- Fraudes.
- Extorsiones.
- Afectaciones a la información.
- Propiedad intelectual.
- Privacidad.

Por lo cual los empleados al ver cualesquiera anomalías en su entorno de trabajo deben reportar lo más pronto posible a la Gerencia o al Oficial de Seguridad de la información mediante un informe de incidente.

INFORME DE REGISTRO DE INCIDENTES DE SEGURIDAD

(Este informe debe ser hecho después del incidente con el objetivo de proporcionar suficientes detalles exactos del incidente para el análisis posterior del mismo. Debe prepararse tan pronto como sea posible, en un entorno tranquilo y seguro. Cada persona involucrada debe preparar un informe individual.)

Tipo de incidente de seguridad: _____

Localización geográfica exacta: _____

Descripción física del lugar: _____

Fecha: _____ Día: _____ Hora: _____

Identificación de todas las personas involucradas: _____

_____

Cómo ha ocurrido el incidente:

_____

_____

_____

Descripción del incidente:

_____

_____

_____

Acciones y decisiones tomadas y por quién:

_____

_____

_____

Reacciones de otros:

_____

_____

_____

Se ha llevado a cabo alguna acción inmediata:

_____

_____

_____

Fecha y lugar: _____ Entregado por: _____

Firma: _____

Fuente: Guide to Cash-for-Work Programming (2006) Mercy Corps

- **Fraudes.**

  La organización deberá contar con un plan de prevención contra el fraude el cual deberá tener los siguientes elementos:

  a) Análisis y Monitoreo de los riesgos del Fraude
  b) Segregación de las responsabilidades de los riesgos identificados
  c) Evaluación Permanente
  d) Establecimiento de Políticas que manejen los eventos de Fraude
  e) Análisis de los controles que mitiguen los riesgos ocasionados por el Fraude
  f) Mejora Continua
  g) Planes proactivos para detección de fraudes

Los empleados deben reportar cualquier actividad sospechosa de Fraude mediante correo electrónico o llamada al Gerente o al área legal quien normalmente se encargan de investigar y recibir este tipo de casos. Para comunicar estos incidentes se utiliza el INFORME DE REGISTRO INCIDENTES. La necesidad de requerir análisis forense para una investigación más detallada

- **Extorsiones.**

Se debe tener las medidas necesarias para prevención para evitar cualquier incidente de extorsión y es por ello que la Gerencia mediante capacitaciones deben orientar a sus empleados a no brindar información por cualquier medio vía teléfono o encuestas para así evitar los incidentes de extorsión. Si llegase a dar el caso de extorsión entonces lo que se debería hacer es comunicar el incidente y realizar el INFORME DE REGISTRO DE INCIDENTES lo más pronto posible. El área de TI y encargado de Seguridad y el Área Legal, deberá colaborar con la investigación del incidente y aportar los datos necesarios para su mitigación y solución

- **Afectaciones a la información.**

Para ello la empresa debe tener una metodología o una gestión de seguridad de la información con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información de sus sistemas de información con lo cual debe tener todos los mecanismos y controles para la protección de los activos. Para prevenir incidentes como la fuga de la información o cualquier incidente que afecte la integridad de la información la organización deberá:

- Conocer la información que gestiona y controla la organización.
- Clasificar la información según su criticidad y grado de riesgo a las que está expuesta.
- Determinar el grado de seguridad con lo que cuenta.
- Establecer las medidas de seguridad necesarias.

<u>Medidas de seguridad.</u>

- Mantener cifrada la información
- Instalación y actualización de un Cortafuegos
- Mantener siempre actualizadas en su última versión las aplicaciones de los sistemas que se utilicen.
- Monitorización y Control para prevención de pérdidas de datos

- Herramientas de control de los dispositivos externos que se utilizan.
- Fijar Políticas de Seguridad junto con la debida concientización y capacitación a los empleados.
- Es importante que los empleados firmen un acuerdo de confidencialidad y cumplimiento de las políticas de seguridad de la organización.

Si llegase a dar el caso de algún incidente de Afectaciones a la información entonces lo que se debería hacer es comunicar el incidente y realizar el INFORME DE REGISTRO DE INCIDENTES lo más pronto. El área de TI y encargado de Seguridad y el Área Legal, deberá colaborar con la investigación del incidente y aportar los datos necesarios para su mitigación y solución

- **Propiedad intelectual.**

El área de TI es el encargado de supervisar y monitorear que todos los sistemas que se utilicen en la organización estén eficazmente configurados, actualizados y con sus licencias legalmente adquiridos, además de la misma manera los empleados deben respetar las políticas de seguridad de la organización y de no usar programas externos sin licencias para evitar cualquier incidente que tenga que ver con la propiedad intelectual. La organización debe tener una política de prohibición de uso de programas que no cuenten con una licencia y descargas de contenidos como ser el uso de torrents.
La organización debe contar con ciertas reglas para prevenir controversias con empleados o contratistas independientes:

- Disponer con asesoramiento jurídico
- Celebrar acuerdos por escrito
- Establecer contratos antes de que se inicien cualquier trabajo
- Siempre incluir clausulas de confidencialidad en los acuerdos y contratos
- Tomar precauciones al subcontratar actividades de investigación y desarrollo

El área legal es la encargada de mitigar y tratar los incidentes con respecto a la propiedad intelectual, siempre con el apoyo de las áreas de TI y de seguridad.

- **Privacidad.**

El área de auditoria será el encargado de realizar las respectivas actividades de monitoreo y evaluación del cumplimiento de los controles y mecanismos de protección que garanticen la confidencialidad, integridad y disponibilidad de la información. Las medidas que se deberán realizar para evitar la divulgación de información de la organización es tener políticas y que los empleados las cumplan:

- Mantener los dispositivos y equipos físicos y lógicos actualizados
- Protección frente accesos no autorizados
- Cifrado de la información
- Gestión de contraseñas
- Detección de accesos

El área legal, TI y de Seguridad deberán encargarse de darle seguimiento e investigar los incidentes con este tipo de delito.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El área responsable de recibir y atender los incidentes de seguridad de la información de la organización debe manejar los niveles de criticidad de los eventos y clasificarlos para asi darle el tratamiento adecuado.

Niveles de Riesgo

EVALUACIÓN DEL RIESGO - NIVEL DEL RIESGO		OPCIONES DE GESTIÓN DEL RIESGO / EN FUNCIÓN DEL NIVEL DEL RIESGO ADMISIBLE
	BAJO	* Asumir el riesgo
	MEDIO	* Reducir el Riesgo
	ALTO	* Evitar el Riesgo.

		* Compartir o transferir el riesgo
	MUY ALTO O CRÍTICO	* Reducir el Riesgo * Evitar el Riesgo. * Compartir o transferir el riesgo

Clasificación de Incidentes

Nivel de Riesgo	Incidentes	Responsable
Crítico	Afectaciones a la información • Gusano/Virus/Troyano/Spyware • Software instalado intencionalmente para realizar actividades maliciosas.	T. I. / Legal
	Privacidad • Acceso no autorizado • Robo de Información	Legal
Alto	Afectaciones a la información • Negación de Servicios	Seguridad
Medio	Propiedad intelectual - • Instalación de software ilegal	T. I
Bajo	Fraude • Intento de uso no autorizado de cuentas bancarias, sin ninguna afectación.	Legal

ACTIVIDADES PARA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- Reportar Incidentes de Seguridad
- Registrar los eventos e incidentes
- Evaluar el impacto de los incidentes
- Identificar la relevancia de la información / activos
- Establecer estrategias para respuesta de acción de los incidentes de seguridad
- Implementar las medidas de seguridad
- Estrategias de contención
- Recolección de evidencias
- Manejar las evidencias
- Identificación de las fuentes de ataques
- Establecer estrategias de erradicación y tratamiento
- Aplicar procedimientos de recuperación
- Realizar análisis post-incidentes

CONCLUSIONES

Es importante que todas las organización estén bien preparados contra cualquier tipo de incidentes de seguridad ya que hoy en día mediante el internet y avances tecnológicos aumenta la brecha a ataques informáticos a los sistemas de información, es por ellos que se debe tener un plan de acción de manejo de incidentes ya sea para detección, prevención y tratamiento de los riesgos y así la organización pueda responder a cualquier tipo de ataques y salir bien libradas sin tener ninguna perdida grave en sus activos importantes. También hay que mencionar que la organización debe tener una cultura donde sus políticas de seguridad sean comprendidas por todos los empleados y haya compromiso de cumplirlas y denunciarlas y las áreas responsables hagan el seguimiento indicado para resolverlo.