Asignatura	Datos del alumno	Fecha
Seguridad en Entornos Móviles y Virtualización	Grupo 29 Ángel Ramon Paz López Blanca Paola Toledo Martínez Braulio David Velasco Castillo	01.08.2022

Trabajo Grupal: Desarrollar mecanismos de protección contra riesgos provocados por la fuga de información

1	**Fase inicial**	Detección del incidente Alerta del incidente a nivel interno Inicio del protocolo de gestión
2	**Fase de lanzamiento**	Reunión del gabinete de crisis Informe inicial de situación Coordinación y primeras acciones
3	**Fase de auditoria**	Auditorio interna y externa Elaboración de informe preliminar
4	**Fase de evaluación**	Reunión del gabinete Presentación del informe de auditoria Determinación de principales acciones Tareas y planificación
5	**Fase de mitigación**	Ejecución de todas las acciones del plan
6	**Fase de seguimiento**	Valoración de los resultados del plan Gestión de otras consecuencias Auditoria completa Aplicación de medidas y mejoras

Asignatura	Datos del alumno	Fecha
Seguridad en Entornos Móviles y Virtualización	Grupo 29 Ángel Ramon Paz López Blanca Paola Toledo Martínez Braulio David Velasco Castillo	01.08.2022

Fase de evaluación

En esta fase el equipo del gabinete de crisis inicia el proceso de evaluación del incidente suscitado como ser las consecuencias y el impacto, tomando como punto de partida la información recopilada y estudiada en las fases pasadas lo que es la detección del incidente, informes de situación actual, informe preliminar de auditoria entre otras actividades, como lo podemos visualizar.

Consecuencias e impacto

- Dañar la imagen de la empresa
- Desconfianza en los clientes y proveedores.
- Afectación a terceras personas, usuarios externos que confiaban en la empresa y sus datos personales son revelados al público.
- Consecuencias Legales
- Consecuencias Económicas

Causas

- No hay una clasificación de la información.
- Falta de conocimiento por parte de los empleados de la empresa
- No hay políticas ni procedimientos de protección de los datos
- No hay acuerdos de confidencialidad de la información con los empleados
- No hay controles ni mecanismos de protección en los dispositivos electrónicos que se utilizan en la empresa, como controles de acceso, controles y prevención de malware entre otros.

Tareas y Acciones

- Conocer el valor de la información y clasificarla según su confidencialidad
- Concientización y capacitación del valor de la información y aplicación de responsabilidades
- Implementación de herramientas tecnológicas para protección de la información
- Implementación de políticas, procedimientos y estándares que permitan reducir, mitigar los riesgos a las que está expuesta la empresa.
- Tareas de actuación con los afectados una vez que un incidente se lleve a cabo.
- Tareas de mitigación y prevención con el objetivo de repeler las consecuencias que pueda ocasionar la fuga de información.

- Tareas de análisis y evaluación de riesgos.
- Planificación de comunicación e información del incidente tanto con las personas afectadas como con las organizaciones competentes.

Mecanismos preventivos para la mitigación del impacto

- Realizar revisiones periódicas a las tareas y acciones acordadas en busca de mejora continua
- Contar con respaldos de información
- Actualización de los sistemas
- Antivirus
- Firewalls
- Navegación en internet segura
- Contraseñas con estándares seguros
- Accesos remotos
- Roles y permisos

Mecanismos correctivos para la mitigación del impacto

- Catalogar y asignar los problemas e incidentes
- Analizar los problemas
- Analizar las soluciones
- La documentación del incidente

Mecanismos detectables para la mitigación del impacto

- Detección del punto exacto del ataque
- Detección de las actividades sospechosas y conocimiento de lo sucedido
- Realizar las actividades pertinentes para la solución, mitigación del impacto y resolución del incidente
- Documentación

Los elementos que acompañan al tratamiento y mitigación de los riesgos es contar con los siguientes programas:

- Programa de gestión de activos
- Programa de gestión de configuración
- Programa de gestión de cambio

Asignatura	Datos del alumno	Fecha
Seguridad en Entornos Móviles y Virtualización	Grupo 29 Ángel Ramon Paz López Blanca Paola Toledo Martínez Braulio David Velasco Castillo	01.08.2022

Planes de seguridad

Nombre del Plan	**Implementación de políticas de acceso.**
Objetivo	Protección de la información de personas ajenas de la empresa o área asignando roles y permisos de usuario.
Riesgos tratados	Afectación a la integridad, confidencialidad y disponibilidad de la información. Accesos no autorizados Suplantaciones de usuarios
Responsables	Seguridad de la información, Administrador del sistema, Gabinete de crisis
Actividades	El Administrador del sistema será el único responsable de creación de usuario y modificación de información Usuarios que son inactivos y que llevan un periodo de tiempo sin actividad sean eliminados Asignar los permisos de usuarios lo mínimos posible a cada usuario otorgando los permisos necesarios para realizar la función correspondiente a cada área. Mantener logs para auditoria Las contraseñas de usuarios deben cumplir con las políticas de contraseña segura, al no cumplir este requisito el sistema debería rechazar la creación de la cuenta. Los sistemas no deben permitir iniciar varias sesiones con un mismo usuario

Nombre del Plan	**Concientización y capacitaciones de seguridad informática**
Objetivo	Enseñar y mostrar a los empleados de la empresa la importancia de la seguridad informática y generar una cultura de seguridad de la información
Riesgos tratados	Afectación a la integridad, confidencialidad de la información. Suplantaciones de usuarios Robo de información
Responsables	Seguridad de la información, Gabinete de crisis
Actividades	Capacitación a los empleados de la empresa Talleres de sensibilización y ejemplos prácticos de como un hacker puede burlar la seguridad de la empresa mediante el phishing.

Asignatura	Datos del alumno	Fecha
Seguridad en Entornos Móviles y Virtualización	Grupo 29 Ángel Ramon Paz López Blanca Paola Toledo Martínez Braulio David Velasco Castillo	01.08.2022

Nombre del Plan	**Gestión de respuestas a incidentes, Gabinete de crisis**
Objetivo	Actuar de forma inmediata a cualquier incidente que se materialice en la empresa.
Riesgos tratados	✓ Afectación a la integridad, confidencialidad y disponibilidad de la información. ✓ Explotación y penetración de vulnerabilidades
Responsables	Seguridad de la información
Actividades	✓ Implementar políticas y procedimientos asignando responsables con el fin de realizar una gestión de incidentes y comunicar resultados a la gerencia de la empresa. ✓ Elaborar planes de respuestas ✓ Procedimientos de mitigación y seguimiento de los incidentes y vulnerabilidades a las que está expuesta la empresa con sus respectivos reportes. ✓ Procedimiento de evaluación y prevención con sus respectivos reportes de auditoría. ✓ Planes de recuperación por cualquier incidente negativo que pudiese materializarse y afectar la disponibilidad de los servicios de la empresa. ✓ Comunicar todo tipo de reportes a la gerencia de la empresa.

Nombre del Plan	**Plan de comunicación de incidentes.**
Objetivo	Informar a la gerencia todo informe de afectación de incidentes materializados en la empresa e informar a los afectados externos dependiendo el nivel de criticidad para que tomen acciones de seguridad con su información.
Riesgos tratados	Afectación a la integridad, confidencialidad y disponibilidad de la información.
Responsables	Seguridad de la información, Gabinete de crisis
Actividades	Seleccionar un proceso de comunicación Describir la frecuencia de comunicación y las herramientas que se usuran en la comunicación. Seleccionar el tipo de público a la cual se estará comunicando la información Encargado y responsable de la comunicación. 1008070

Des pues de todo lo antes mencionado es necesario tomar en cuenta que después de fuga de información es de suma importancia cortar y evitar nuevas fugas de información, así como la revisión de la propagación de la información y la atenuación de la misma, sobre todo si esta cuenta con información confidencial, proceder con los perjudicados por la fuga de información aunque estos sean ajenos a la organización y proceder a la mitigación de las consecuencias legales y preparar la información que sea

requerida para una posible denuncia con los afectados y de esta manera poder proceder a las consecuencias económicas que pudieran perjudicar a la organización y de esta manera proceder a su mitigación, la planificación de comunicación e información de la eventualidad de manera interna, externa y medios de comunicación en caso de ser necesario.

Indica en la actividad el nombre de todos los componentes del equipo y cumplimenta la siguiente tabla de valoración individual:

	Sí	No	A veces
Todos los miembros se han integrado al trabajo del grupo	X		
Todos los miembros participan activamente	X		
Todos los miembros respetan otras ideas aportadas	X		
Todos los miembros participan en la elaboración del informe	X		
Me he preocupado por realizar un trabajo cooperativo con mis compañeros	X		
Señala si consideras que algún aspecto del trabajo en grupo no ha sido adecuado		X	

REFERENCIAS

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_fuga_informacion_0.pdf

(2022). Retrieved 1 August 2022, from https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Toro, R. (2022). ISO 27001: Plan de tratamiento de riesgos de seguridad de la información. Retrieved 1 August 2022, from https://www.pmg-ssi.com/2017/06/iso-27001-plan-tratamiento-riesgos-seguridad-informacion/#:~:text=Por%20esto%2C%20el%20plan%20de,la%20informaci%C3%B3n%20para%20sus%20operaciones.

Asignatura	Datos del alumno	Fecha
Seguridad en Entornos Móviles y Virtualización	Grupo 29	01.08.2022
	Ángel Ramon Paz López Blanca Paola Toledo Martínez Braulio David Velasco Castillo	

Metodología

Para ello se elaborarán dos tablas: una para la institución pública y otra para la institución privada. En ellas se determinarán los componentes/*bullets* que deben ser considerados durante la planeación, las tareas, las acciones y la ejecución, que ayuden a resolver los incidentes respecto a las fugas de información, al tiempo que se resaltan los pros y los contras de cada una de ellas.

Se sugiere investigar a partir de la información aportada en las ideas claves del tema y de la bibliografía existente, que describe el rubro de fugas de información en el tema «Características avanzadas de seguridad en entornos móviles y virtuales», documentado por UNIR.

Extensión máxima: cinco páginas, con fuente Georgia 11 e interlineado 1,5.