pirani

Módulo 4

Eventos, incidentes y dominios de control

CONTENIDO

1. Eventos e incidentes de seguridad de la información

1. Implementación de controles

1.

Eventos e incidentes de seguridad de la información

¿Qué es un evento y qué es un incidente?

Evento

Presencia identificada de una condición de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información.

Incidente

Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Tipos de incidentes

Tecnológico

Incidentes que afectan la disponibilidad, confidencialidad o integridad de las tecnologías de información. Algunos ejemplos son:

- Denegación de servicio.
- Código malicioso.
- Acceso no autorizado a los sistemas de información.
- Fallas en los sistemas de información.

No Tecnológico

Aquellos incidentes que su causa no obedece a factores tecnológicos, por ejemplo:

- Violaciones de confidencialidad, disponibilidad e integridad de documentos.
- Filtración de información reservada.
- Incidentes provocados por la naturaleza.
- Incumplimiento de las políticas o directrices del SGSI.
- Violaciones de seguridad física.

¿Cómo actuar ante un evento?

Acciones de TI

- Bloqueo de dominios
- Actualización del antivirus
- Reforzar medidas de seguridad

Acciones del colaborador / usuario

- Aplicar las recomendaciones
- Subir el nivel de seguridad propio
- Realizar Backups
- Estar alerta

¿Cómo actuar ante un incidente?

Acciones conjuntas TI + Colaborador + Oficial SGSI

Vacunar el equipo de cómputo

Medir el impacto

Datos personales

- Revisar los datos afectados
- Tomar medidas para proteger los datos expuestos
- Notificar a los titulares (si aplica)
- Notificar a la SIC.

Información

- Ejecutar herramientas de escaneo de la red, servidores.
- Asegurar la información
- Restaurar backup
- Medidas para restaurar la confidencialidad, integridad y disponibilidad.

2.
Implementación de controles

Implementación de controles

Políticas

Todo el personal, proveedores y terceros deben velar por la protección de la información de la entidad y de los clientes, así como el uso seguro del ciberespacio, objetivo que debe estar enmarcado en los principios de confidencialidad, integridad y disponibilidad.

- Alta Gerencia.
- Objetivos estratégicos.
- Regulaciones y leyes.

Organización

Todos los funcionarios y terceros hacen parte de una estructura organizacional de seguridad donde se debe contar con roles y responsabilidades.

Se debe dar cumplimiento a procedimientos y controles que garanticen el logro de los objetivos de Seguridad de la Información. En dicha estructura se deben considerar todos los proyectos o procesos que se ejecuten y los medios o dispositivos de acceso a la información.

Implementación de controles

Recursos humanos

Colaboradores contratados directamente o por un proceso de tercerización deben velar por el cumplimiento de los objetivos y las políticas de la Seguridad de la Información.

- Proceso de selección.
- Contratación.
- Formación.
- Toma de conciencia.
- Cambios de cargo.

Antes, durante y después.

Gestión de activos

La información constituida por aquella que es suministrada por los clientes y la concerniente a los procesos propios de negocio es considerada como esencial.

- Identificar claramente los activos de información.
- Identificar su rol como dueños o custodios.
- Clasificarse a fin de definir su importancia para la organización.
- Protegerse independientemente del medio en el que se encuentre o transmita.

Implementación de controles

Control de acceso

Los aplicativos, sistemas operativos, redes y demás recursos tecnológicos deben contar con requerimientos y esquemas de control de acceso confiables.

- Resguardar apropiadamente las credenciales que le son suministradas.
- Procesos de gestión de acceso de usuarios y perfiles.
- Responsabilidad y el control de acceso de los usuarios.

Criptografía

Controles criptográficos para la protección de la información siendo necesario emplearlos en el establecimiento de canales de comunicación, protección de los activos con información confidencial y sensible.

- Mecanismos usados para mantener la confidencialidad, disponibilidad y la integridad de la información.
- Las llaves o componentes criptográficos deberán ser usados y protegidos por los dueños o administradores en todo su ciclo de vida.

Implementación de controles

Seguridad física y ambiental

Las instalaciones deben ser protegidas de amenazas tanto internas como externas, en especial zonas que se consideran restringidas y que resguardan equipos de procesamiento de información o documentación confidencial y/o sensible.

- Perímetro de seguridad,
- Control de acceso.
- Seguridad en oficinas y puestos de trabajo.
- Protección contra amenazas internas y externas.
- Seguridad en todas las áreas que se considere que manejen información.

Seguridad en las operaciones

Los sistemas tecnológicos propios o de terceros que manejan información deben tener procedimientos operacionales, responsabilidades, y ser protegidos de riesgos.

- Software malicioso.
- Aprovechamiento de vulnerabilidades,
- Pérdida de información.
- Cambios no controlados.

Cada área deberá velar por la confidencialidad, integridad y disponibilidad en estos, realizando registro y seguimiento.

Implementación de controles

Seguridad en las comunicaciones

Las comunicaciones se deben realizar por medio de los dispositivos dispuestos y en el marco de las funciones laborales de cada área, por esto la información que viaja o se transfiere a través de las redes es protegida por medio de mecanismos que controlan, limitan, cifran y monitorean la información a través de estas. Cualquier conexión con terceros deberá realizarse usando protocolos seguros y acuerdos de confidencialidad para su uso.

Adquisición, desarrollo y mantenimiento de sistemas

Requerimientos de seguridad durante todo el ciclo de vida de los sistemas de información que se adquiera o diseñe.

- Compra
- Adquisición de nuevas tecnologías
- Desarrollo seguro
- Mantenimiento y baja
- Riesgos
- Protección de información en tránsito
- Ambientes y datos de prueba
- Pruebas de seguridad
- Revisión de código.

Implementación de controles

Relación con proveedores

Los proveedores deben dar cumplimiento a las políticas de seguridad definidas y por la normatividad vigente en el ámbito del servicio prestado y la cadena de suministro.

- Mecanismos de seguridad para la gestión, seguimiento y revisión de los servicios contratados,
- Proteger la información a la que tienen acceso los proveedores manteniendo la confidencialidad y la integridad de la misma.

Gestión de incidentes

Todos los terceros, funcionarios y especialmente administradores y áreas de control deben realizar reporte de debilidades, eventos e incidentes que hayan sido identificados para que cada caso sea priorizado y gestionado en procedimiento de gestión de incidentes de seguridad de la información.

- Reporte.
- Análisis.
- Evaluación.
- Respuesta.
- Evidencias.
- Lecciones aprendidas.
- Mejora continua.

Implementación de controles

Seguridad de la información en continuidad del negocio

Se debe contar con planes de contingencia y continuidad del negocio que consideren en su ejecución el cumplimiento de las Políticas de Seguridad y Ciberseguridad, así como la inclusión de escenarios de ciberseguridad para garantizar el plan de continuidad de negocio antes, durante y después de sucedido el evento, y las regulaciones aplicables.

- Garantizar la seguridad de la información en ambientes tanto productivos como de contingencia.
- Durante el tiempo de permanencia.
- Incluyendo el retorno a la normalidad.

Cumplimiento

Todas las áreas y terceros deben cumplir con las políticas y con las obligaciones legales, estatutarias, de legislación, reglamentación o contractuales que apliquen en cuanto a la Seguridad de la Información.

Las áreas de control internas o contratadas podrán verificar de forma independiente y en cualquier momento o de manera periódica el cumplimiento de normatividad o regulaciones aplicables en términos operacionales, funcionales y técnicos.

¡Gracias!

pirani | www.pirani.co/es