Tarea 1 : CiberGobierno

Panama

Colombia

Republica Dominicana

Ecuador

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Cyber Gobierno

Inteligencia de Amenazas

Security Operations Center (SOC)

Desarrollo de procesos y políticas: *Establecer políticas y procedimientos de seguridad operativa para: supervisión de eventos, respuesta a incides y recuperación.*

Capacitación del equipo: *capacitación continua para los analistas y el personal de SOC sobre las últimas amenazas y técnicas de mitigación. Certificación del personal en las soluciones de seguridad desplegadas.*

Renovación tecnológica: *Adquisición de herramientas internas o servicios administrados o licenciamiento necesario.*

Seguridad Digital

- ***Estrategia:***

Defensa en profundidad.

- *Establecer políticas y procedimientos de seguridad asociados a cada apartado de la implementación.*
- *Garantizar el cumplimiento de las regulaciones y estándares del apartado de cumplimiento.*
- ***Implementación en Profundidad:***
  - *Defensa perimetral y WAF*
  - *Segmentación de red*
  - *Seguridad de la red*
  - *Control de acceso a la red (NAC)*
  - *Seguridad en endpoint (EDR)*
  - *Cifrado, DLP, IAM, MFA,*

Centro de Excelencia (CoE)

Implementación de los siguientes planes:

Respuesta a incidentes y Recuperación de desastres:

- *Desarrollar y actualizar periódicamente un plan de respuesta a incidentes /recuperación de desastres*
- *Establecer un equipo de respuesta a incidentes (IRT) dedicado dentro del equipo de seguridad.*
- *realizar pruebas de escritorio de recuperación, simulacros y simulaciones.*
- *Concientización y capacitación de usuarios.*
- ***Auditoría y Mejora continua***

Respuesta a Incidentes

Regulaciones de Gobierno y Globales

REGULACIÓN APLICABLE

Para empresas de México:

- *LFPDPPP, GRDP (para clientes o proveedores de UE)*

IMPLEMENTACIÓN

1. Diagnóstico y Evaluación Inicial

2. Determinar las obligaciones legales específicas según la LFPDPPP.

3. Capacitación y Concienciación

EVALUACIÓN DE LA IMPLEMENTACIÓN

Realizar evaluaciones de impacto en la privacidad para nuevos proyecto.

MANTENIMIENTO Y ACTUALIZACIÓN

Revisar y actualizar regularmente las políticas, procedimientos y medidas de seguridad.

DOCUMENTACIÓN

Documentar cada una de las etapas del proceso, de las láminas anteriores.

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Inteligencia de Amenazas

Agregar acá la información de cómo manejarás la Inteligencia de Amenazas.

Ej.: Herramienta o conjunto de herramientas, Algoritmos, etc.

- ***Estratégico:*** *La inteligencia estratégica sobre amenazas es información de alto nivel que pone la amenaza en contexto. Implementación de una herramienta GRC automática que ayude a la tarea operativa de realizar el levantamiento y sobre todo, el seguimiento de un nuevo riesgo: https://www.cybersaint.io/glossary/what-is-a-grc-tool*
- ***Táctica:*** *La inteligencia táctica sobre amenazas incluye los detalles de cómo se llevan a cabo y se defienden las amenazas, incluidos los vectores de ataque, las herramientas y las infraestructuras que utilizan los atacantes, los tipos de empresas o tecnologías a las que se dirigen y las estrategias para evitarlas. Contratación de un servicio de inteligencia de Amenazas como servicio Administrado por un vendor que entregue a la organización de manera mensual, un reporte con la información de amenazas identificadas para el giro de la organización:*
  https://www.eset.com/fileadmin/ESET/INT/Products/Business/Services/Threat_Intelligence/ESET_Threat_Intelligence_product_overview-NEW.pdf
- ***Operacional:*** *la inteligencia operativa sobre amenazas es información que un departamento de TI puede utilizar como parte de la gestión activa de amenazas para tomar medidas contra un ataque específico. Designar una tarea específica al equipo para correlacionar el análisis de riesgo con el reporte de Inteligencia de Amenazas, así que de manera mensual, se priorize el esfuerzo en mitigar el riesgo detectado como prioritario.*
- ***Técnico:*** *La inteligencia técnica sobre amenazas es evidencia específica de que se está produciendo un ataque o indicadores de compromiso (IOC). Implementación de NDR para detección y contención de amenazas de red https://darktrace.com/products/network/detect-respond*

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Security Operations Center (SOC)

Agregar acá la información de cómo manejarás el Security Operations Center

Ej.: Cuales procesos, herramientas y tecnologías usarán para manejar el Security Operations Center

El SOC Debe de tener por lo menos, los procesos, herramientas y tecnologías listadas. Se evaluarán proveedores y también, la implementación de forma interna mediante la medición de objetivos con las áreas de Staff involucradas:

GENERAL

- ***Desarrollo de políticas:*** *Establecer políticas y procedimientos de seguridad operativa.*
- ***Capacitación del equipo:*** *capacitación continua para los analistas y el personal de SOC sobre las últimas amenazas y técnicas de mitigación.*
- ***Renovación tecnológica:*** *Adquisición de herramientas internas o servicios administrados o licenciamiento necesario.*

PROCESOS

Supervisión (Procesos/Procedimientos)

- ***Recopilación de datos****: Procesos de Registros y datos de seguridad de diversas fuentes (servicios administrados, licenciamiento pago).*
- ***Monitoreo en tiempo real:*** *Monitoreo continuamente eventos y alertas de seguridad utilizando SIEM y otras herramientas de monitoreo.*
- ***Integración de inteligencia de amenazas:*** *Inteligencia de amenazas para mantenerse actualizado sobre amenazas nuevas y emergentes.*

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Security Operations Center (SOC)

Agregar acá la información de cómo manejarás el Security Operations Center

Ej.: Cuales procesos, herramientas y tecnologías usarán para manejar el Security Operations Center

Supervisión (Procesos)

- ***Detección de anomalías:*** *Proceso para la identificación de desviaciones del comportamiento normal que puedan indicar un incidente de seguridad.*
    - ***Desarrollo de casos de uso:*** *Proceso de creación y mantenimiento de casos de uso de detección para identificar amenazas identificadas para la rama de negocio.*
    - ***Correlación y análisis:*** *correlacione eventos y analice datos para detectar posibles incidentes de seguridad.*

Respuesta a incidentes (Procesos)

- ***Triage:*** *Proceso de evaluación y priorización de incidentes en función de su gravedad e impacto potencial.*
- ***Investigación:*** *realizar un análisis en profundidad para comprender la naturaleza y el alcance del incidente.*
- ***Contención:*** *Tome medidas inmediatas para contener la amenaza y evitar daños mayores.*
- ***Erradicación:*** *Eliminar la amenaza del medio ambiente.*

Recuperación (Procesos)

- ***Restauración del sistema:*** *Restaurar los sistemas afectados a su funcionamiento normal.*
- ***Recuperación de datos:*** *recupere datos perdidos o comprometidos a partir de copias de seguridad.*

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Security Operations Center (SOC)

Agregar acá la información de cómo manejarás el Security Operations Center

Ej.: Cuales procesos, herramientas y tecnologías usarán para manejar el Security Operations Center

Recuperación (Procesos)

- ***Verificación:*** *Verifique que la amenaza haya sido completamente erradicada y que los sistemas sean seguros.*
- ***Actividades posteriores al incidente:*** *Proceso de lecciones aprendidas*

TECNOLOGÍA

Preparación: *Dependiendo del presupuesto, contratos, licenciamiento, interconexión y tamaño de la infraestructura se evaluarán los siguientes vendors:*

Herramientas e infraestructura:

- ***Security Information and Event Management (SIEM) SystemsExamples:*** *Splunk*
- ***Endpoint Detection and Response (EDR) :*** *CrowdStrike Falcon, Carbon Black, SentinelOne, Microsoft Defender for*
- ***Threat Intelligence Platforms (TIP):*** *ThreatConnect, Anomali, Recorded Future,*
- ***Vulnerability Management Tools:*** *OpenVAS (2da etapa de la implementación)*
- ***Identify and manage vulnerabilities in the IT environment:*** *Darktrace, Vectra, Extra*
- ***Security Orchestration, Automation, and Response (SOAR) Platforms****: Palo Alto Networks Cortex XSOAR, Splunk Phantom, IBM Resilient, Demisto*

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Security Operations Center (SOC)

Agregar acá la información de cómo manejarás el Security Operations Center

Ej.: Cuales procesos, herramientas y tecnologías usarán para manejar el Security Operations Center

TECNOLOGÍA

Preparación: *Dependiendo del presupuesto, contratos, licenciamiento, interconexión y tamaño de la infraestructura se evaluarán los siguientes vendors:*

- ***Log Management Solutions:*** *Elasticsearch, Logstash, Kibana (ELK Stack), Graylog (2da etapa de implementación)*
- ***Firewall and Next-Generation Firewall (NGFW):*** *Cisco ASA, Palo Alto Networks, Check Point, Fortinet FortiGate*
- ***Email Security Solutions****: Proofpoint, Mimecast, Microsoft Defender for Office 365, Symantec Email Security.cloud*
- ***Web Application Firewalls (WAF):*** *AWS WAF, Cloudflare, Imperva, Akamai Kona Site Defender.*
- ***Data Loss Prevention (DLP):*** *Symantec DLP, McAfee Total Protection for DLP, Forcepoint DLP, Digital Guardia*
- ***Identity and Access Management (IAM):*** *Okta, Microsoft Azure AD, IBM Security Identity Manager, RSA SecurID*
- ***Endpoint Protection Platforms:*** *Symantec Endpoint Protection, McAfee Endpoint Security, Sophos Intercept X, Trend Micro Apex One*
- ***Cloud Security Solutions:*** *Prisma Cloud, AWS Security Hub, Microsoft Azure Security Center, Google Cloud Security Command Center. (2da. Etapa de la implementación)*
- ***Incident Response Tools:*** *Carbon Black Response, FireEye HelixAssist in managing and responding to security incidents.*
- ***Patch Management Tools:*** *Microsoft SCCM, Ivanti Patch Management, SolarWinds Patch Manager, ManageEngine.*

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Seguridad Digital

Agregar acá la información de cómo manejarás la Seguridad Digital

Ej.: Cuales procesos, herramientas y tecnologías usarán para manejar la Seguridad Digital.

GENERAL

La estrategia de seguridad digital seleccionada debido al despliegue y soluciones utilizadas para SOC será despliegue de ***defensa en profundidad,*** *ya que la renovación tecnológica propuesta en el modelo de actualización del SOC lo permite. La estraegia de seguridad Digital también se encontrará alineada a ISO27002:2022 para el apartado de controles teconólogicos.*

IMPLEMENTACIÓN

1. ***Establecer políticas y procedimientos de seguridad*** *asociados a cada apartado de la implementación (a-h)*
2. ***Cumplimiento****: Garantizar el cumplimiento de las regulaciones y estándares del apartado de cumplimiento.*
3. ***Implementación en Profundidad:***
   a) ***Defensa perimetral:*** *Implementar firewalls para controlar el tráfico de red entrante y saliente, sistemas de detección/prevención de intrusiones (IDS/IPS): implemente IDS/IPS para detectar y prevenir actividades maliciosas.*
   b) ***Firewalls de aplicaciones web (WAF):*** *implementación de WAF para proteger las aplicaciones web de amenazas comunes.*
   c) ***Segmentación de red:*** *para limitar la propagación de ataques.*
   d) ***Seguridad de la red:*** *Implementación de VPN para un acceso remoto seguro.*
   e) ***Control de acceso a la red (NAC):*** *implementación de NAC para controlar los dispositivos que acceden a la red.*

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Seguridad Digital

Agregar acá la información de cómo manejarás la Seguridad Digital

Ej.: Cuales procesos, herramientas y tecnologías usarán para manejar la Seguridad Digital.

IMPLEMENTACIÓN (Continuación)

3. ***Implementación en Profundidad:***
   - ***e) Seguridad en endpoint Antivirus/Anti-Malware:*** *Implementación de antivirus y anti-malware.*
   - ***f) Detección y respuesta de endpoints (EDR):*** *Segunda etapa para implementar EDR para monitorear y responder a amenazas en endpoints.*

PROTECCIÓN DE DATOS (Alineado a la Regulación Aplicable)

- ***a) Cifrado:*** *Implementación de cifrado datos confidenciales, tanto en reposo como en tránsito.*
- ***b) Prevención de pérdida de datos (DLP):*** *implementación de soluciones DLP para evitar la filtración de datos no autorizada.*
- ***c) Gestión de identidades y accesos (IAM)***
- ***d) Autenticación multifactor (MFA):*** *requiere MFA para acceder a sistemas críticos.*
- ***e) Mínimo privilegio:*** *aplique el principio de mínimo privilegio para las cuentas de usuario y de servicio.Controles de acceso: revise y actualice periódicamente los controles de acceso.*

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Centro de Excelencia (CoE)

Agregar acá la información de cómo manejarás la Centro de Excelencia

Ej.: Cuales procesos, planes de capacitación, perfiles de personas, planes de gobierno como : Recuperación a desastres, continuidad de negocios.

ALCANCE

Las acciones de implementación se llevarán a cabo mediante líneas guía de ISO27002 e ISO 22301.

IMPLEMENTACIÓN

Plan de respuesta a incidentes (IRP):

- *Desarrollar y actualizar periódicamente un plan de respuesta a incidentes de acuerdo a las líneas guía de los estándares ISO utilizados como referencia.* (Mayor información en la lámina de Respuesta a incidentes).
- *Equipo de respuesta: Establecer un equipo de respuesta a incidentes (IRT) dedicado dentro del equipo de seguridad.*
- *Simulacros: realizar pruebas de escritorio de recuperación y simulacros de respuesta a incidentes con regularidad.*
    - *Concientización y capacitación de usuarios: Realizar un programa de capacitación periódica en seguridad para todos los empleados.*
    - *Simulaciones de phishing: realice simulaciones de phishing para educar a los usuarios sobre cómo reconocer intentos de phishing.*

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Centro de Excelencia (CoE)

Agregar acá la información de cómo manejarás la Centro de Excelencia

Ej.: Cuales procesos, planes de capacitación, perfiles de personas, planes de gobierno como : Recuperación a desastres, continuidad de negocios.

ALCANCE

Las acciones de implementación se llevarán a cabo mediante líneas guía de ISO27002 e ISO 22301.

IMPLEMENTACIÓN

Evaluación de Riesgos y Análisis de Impacto

a) *Identificar posibles desastres y riesgos que puedan afectar a la organización (esto es una entrada de la implementación de la inteligencia de Amenazas y estrategia de Seguridad Digital).*
b) *Evaluar el impacto potencial de estos riesgos en las operaciones y determinar las funciones críticas mediante un BIA (Análisis de Impacto al negocio.)*

Desarrollo del Plan

a) *Definir los objetivos de tiempo de recuperación (RTO) y los puntos de recuperación (RPO) para cada función crítica.*
b) *Documentar los procedimientos y acciones necesarias para recuperar las operaciones en caso de un desastre.*
c) *Actualizar las políticas de seguridad de manera que abonen a la efectividad de los procedimientos del plan de recuperación*
d) *Incluir detalles sobre la recuperación de sistemas, datos y aplicaciones.*
e) *Establecer el plan de comunicación que involucre a todos los responsables y a todas las áreas de la organización.*

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Centro de Excelencia (CoE)

Agregar acá la información de cómo manejarás la Centro de Excelencia

Ej.: Cuales procesos, planes de capacitación, perfiles de personas, planes de gobierno como : Recuperación a desastres, continuidad de negocios.

IMPLEMENTACIÓN

a) Formar un equipo de recuperación con roles y responsabilidades claramente definidos, con parte del equipo de seguridad operativa y figuras de estrategia: Director de infraestructura, de finanzas, de RRHH, etc.
b) Capacitar al personal sobre sus roles en el DRP

Implementación de Medidas de Recuperación

a) Asegurar que se realicen copias de seguridad regulares y que se almacenen de manera segura.
b) Comprobar que dichas copias de recuperación sirven.
c) Establecer sitios de recuperación alternativos y verificar su disponibilidad.

Pruebas y Simulaciones

a) Realizar pruebas de escritorio regulares del DRP para asegurar su eficacia.
b) Realizar pruebas del plan de comunicación entre áreas a la par de las pruebas de escritorio.
c) Realizar simulaciones de desastres para evaluar la capacidad de respuesta y mejorar el plan.
d) Revisar y actualizar el DRP regularmente para reflejar cambios en la infraestructura y en los riesgos

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Centro de Excelencia (CoE)

Agregar acá la información de cómo manejarás la Centro de Excelencia

Ej.: Cuales procesos, planes de capacitación, perfiles de personas, planes de gobierno como : Recuperación a desastres, continuidad de negocios.

ALCANCE

Auditoría del sistema de gestión de seguridad Implementado mediante líneas guía de ISO27002 e ISO 22301.

IMPLEMENTACIÓN

Plan de Auditoría y Mejora continua

Planificación

a) *Formar un equipo de auditores con las habilidades y conocimientos necesarios.*
b) *Establecer un plan de auditoría interna con periodicidad mínima anual de acuerdo con 19011.*

Implementación

a) *El equipo de auditoría estará encargado de las siguientes acciones, que se llevarán a cabo de acuerdo con lo establecido en el plan de auditoría:*
    - ***Recolección de Información***
        a) *Realizar entrevistas y cuestionarios con el personal clave.*
        b) *Revisar políticas, procedimientos, y registros de seguridad.*
    - ***Evaluación y Análisis***
        a) *Realizar pruebas de vulnerabilidades y evaluaciones técnicas.*

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Centro de Excelencia (CoE)

Agregar acá la información de cómo manejarás la Centro de Excelencia

Ej.: Cuales procesos, planes de capacitación, perfiles de personas, planes de gobierno como : Recuperación a desastres, continuidad de negocios.

IMPLEMENTACIÓN

Plan de Auditoría y Mejora continua

- ***Evaluación y análisis:***
  a) *Evaluar el cumplimiento de la organización con las políticas y normativas de seguridad.*
- ***Informe de Auditoría***
  a) *Documentar los hallazgos, incluyendo vulnerabilidades y áreas de mejora.*
  b) *Proporcionar recomendaciones para mejorar la seguridad.*
  d) *Implementación de Mejoras o plan de trabajo/acción*

EVALUACIÓN Y SEGUIMIENTO

a) *Desarrollar un plan de acción para abordar las recomendaciones del informe de auditoría.*
b) *Monitorear la implementación de las mejoras recomendadas.*
c) *Realizar auditorías periódicas de seguimiento (internas) para asegurar la mejora continua.*
d) *Implementar monitoreo continuo para identificar y responder a nuevas amenazas. (Procesos de SOC)*

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Regulaciones de Gobierno / Globales

Agregar acá la información de a cuales regulaciones estará sujeta

Ej.: Cuales procesos, planes de capacitación, perfiles de personas, planes de gobierno como : Recuperación a desastres, continuidad de negocios.

REGULACIÓN APLICABLE

- *Para empresas de México: LFPDPPP, GRDP (para clientes o proveedores de UE)*

IMPLEMENTACIÓN

1. Diagnóstico y Evaluación Inicial

a) *Realizar una evaluación inicial para identificar los datos personales que se manejan, los procesos involucrados y los riesgos asociados.*

2. Determinar las obligaciones legales específicas según la LFPDPPP.

a) *Designación de un Responsable de Protección de Datos: Nombrar a un responsable de protección de datos (DPO) o crear un comité encargado de la protección de datos dentro de la organización.*
b) *Desarrollo de Políticas y Procedimientos: Crear políticas y procedimientos claros sobre la recolección, uso, almacenamiento, transferencia y destrucción de datos personales.*
c) *Incluir mecanismos para el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).*
d) *Inventario de Datos Personales: Realizar un inventario de todos los datos personales que maneja la organización.*
e) *Clasificar los datos según su nivel de sensibilidad y el riesgo asociado.*

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Regulaciones de Gobierno / Globales

Agregar acá la información de a cuales regulaciones estará sujeta

Ej.: Cuales procesos, planes de capacitación, perfiles de personas, planes de gobierno como : Recuperación a desastres, continuidad de negocios.

IMPLEMENTACIÓN

2. Determinar las obligaciones legales específicas según la LFPDPPP.

g) Mantener registros de los consentimientos obtenidos.
h) Aviso de Privacidad: Elaborar y publicar un aviso de privacidad que cumpla con los requisitos de la LFPDPPP.
i) Asegurar que el aviso de privacidad esté disponible en todos los puntos de recolección de datos personales.
j) Implementar medidas de seguridad técnicas y administrativas para proteger los datos personales contra pérdida, acceso no autorizado, destrucción y alteración.
k) Procedimiento de a las solicitudes de los titulares de manera oportuna y conforme a los plazos establecidos por la ley.

3. Capacitación y Concienciación

a) Capacitar a todos los empleados sobre las políticas y procedimientos de protección de datos personales.
b) Promover una cultura de protección de datos dentro de la organización.
c) Desarrollar y poner en práctica un plan de respuesta a incidentes para manejar violaciones de datos personales.
d) Establecer procedimientos para notificar a las autoridades competentes y a los titulares de los datos en caso de una violación de datos.

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Regulaciones de Gobierno / Globales

Agregar acá la información de a cuales regulaciones estará sujeta

Ej.: Cuales procesos, planes de capacitación, perfiles de personas, planes de gobierno como : Recuperación a desastres, continuidad de negocios.

EVALUACIÓN DE LA IMPLEMENTACIÓN

a) *Realizar evaluaciones de impacto en la privacidad para nuevos proyectos o cambios significativos en el tratamiento de datos personales.*
b) *Documentar y mitigar los riesgos identificados en la implementación y documentación.*
c) *Realizar pruebas y evaluaciones regulares de las medidas de seguridad del resto del sistema de gestión de seguridad.*

MANTENIMIENTO Y ACTUALIZACIÓN

a) *Revisar y actualizar regularmente las políticas, procedimientos y medidas de seguridad.*
b) *Realizar auditorías periódicas para asegurar el cumplimiento continuo de la LFPDPPP.Ejercicio de Derechos ARCOEstablecer mecanismos eficientes para que los titulares de los datos puedan ejercer sus derechos ARCO. Transferencia de Datos Personales.*
c) *Asegurar que cualquier transferencia de datos personales a terceros cumpla con los requisitos legales, incluyendo el consentimiento y las cláusulas contractuales adecuadas.*

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Regulaciones de Gobierno / Globales

Agregar acá la información de a cuales regulaciones estará sujeta

Ej.: Cuales procesos, planes de capacitación, perfiles de personas, planes de gobierno como : Recuperación a desastres, continuidad de negocios.

DOCUMENTACIÓN

a) *Documentar cada una de las etapas del proceso, de las láminas anteriores.*
b) *Mantener una documentación detallada de todos los procesos relacionados con la protección de datos personales:*
   - *Sanciones*
   - *Proceso de garantía de derechos ARCO*
   - *Gobierno de Datos*
   - *Aviso de Privacidad*
c) *Asegurar que todos los registros estén disponibles para auditorías y revisiones por parte de las autoridades competentes.*

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Respuesta a Incidentes

Agregar acá la información de a como manejarás la respuesta a incidentes

Ej.: Cuales procesos, herramientas y tecnologías usarán para manejar la respuesta a incidentes.

ALCANCE

Se define el alcance basado en los controles de ISO 27002, para inicidentes de seguridad informática, la parte tecnológica y de implementación y operacíones de seguridad, van de la mano con la implementación de SOC..

IMPLEMENTACIÓN

Políticas y Procedimientos:

a) *Desarrollar políticas y procedimientos para la gestión de incidentes de acuerdo a ISO 27002 ANEXO A.*
b) *Formar un equipo de respuesta a incidentes con roles y responsabilidades claras.*

Detección y Análisis

a) *Implementar herramientas de monitoreo para detectar incidentes en tiempo real.*
b) *Evaluar y analizar los incidentes para determinar su alcance y gravedad. (TRIAGE)*
c) *Contención, Erradicación y Recuperación de cada incidente*
    - *Contención: Tomar medidas inmediatas para contener el incidente y prevenir su propagación*
    - *.Erradicación: Eliminar la causa del incidente y asegurar que no vuelva a ocurrir.*
    - *Recuperación: Restaurar los sistemas y servicios afectados y verificar su funcionamiento.*

Fátima Rodríguez Giles
01 de Julio 2024

Gobierno de seguridad

Caso de uso: Regulated Privated Companies

Respuesta a Incidentes

Agregar acá la información de a como manejarás la respuesta a incidentes

Ej.: Cuales procesos, herramientas y tecnologías usarán para manejar la respuesta a incidentes.

IMPLEMENTACIÓN

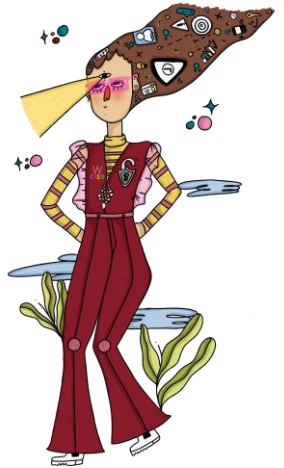
Detección y Análisis

d) Realizar un análisis **post-incidente** *para entender las causas y mejorar la respuesta futura.*
e) Documentar todos los pasos tomados durante la respuesta al incidente.

MEJORA CONTINUA

a) Incorporar las lecciones aprendidas en la política y los procedimientos del IRP.
b) Realizar la actualización tecnológica necesaria para garantizar la efectividad de procesos y procedimientos
c) Realizar un ciclo de auditoría posterior a la incorporación y actualización documental derivada de un incidente de seguridad.
d) Capacitar regularmente al personal sobre nuevos tipos de incidentes y mejores prácticas.

¡Gracias !



WomenCISO Latam
Segunda Generación, 2024