Políticas de securización

30/10/23

Jose Almirón Lopez

Políticas de securización

1. **Control de acceso:**
    - **Política**: Todos los empleados deben usar autenticación de dos factores para acceder a los sistemas críticos.
    - **Procedimiento**: Identificar una solución de autenticación de dos factores adecuada para la empresa, configurarla para todos los empleados y realizar pruebas y ajustes para su funcionamiento adecuado.
    - **Guia**: Instrucciones detalladas sobre cómo identificar, configurar y utilizar la autenticación de dos factores. Incluye pasos claros para la implementación y el uso adecuado en el acceso a sistemas críticos.
2. **Clasificación y manejo de la información:**
    - **Política**: Todos los datos se clasificarán y manejarán según su nivel de confidencialidad y riesgo asociado.
    - **Procedimiento**: Identificar y clasificar los datos según su nivel de confidencialidad. Establecer métodos de protección y manejo acorde a su clasificación. Establecer procedimientos para el acceso, almacenamiento y transmisión segura de la información.
    - **Guia**: Instrucciones detalladas sobre cómo identificar, clasificar y manejar datos según su nivel de confidencialidad. Incluye pautas para el acceso autorizado, almacenamiento seguro y transmisión protegida de la información clasificada.
3. **Seguridad física y ambiental:**
    - **Política**: Mantener medidas de seguridad para proteger las instalaciones y el entorno físico de la empresa.
    - **Procedimiento**: Establecer un plan de seguridad física que incluya control de accesos, cámaras de vigilancia, protocolos de emergencia y mantenimiento de las instalaciones. Asimismo, implementar medidas para minimizar riesgos ambientales que puedan afectar la infraestructura.
    - **Guia**: Instrucciones detalladas para el control de acceso, manejo de cámaras de vigilancia, procedimientos de emergencia y mantenimiento de las instalaciones. También, se incluyen directrices para identificar y mitigar riesgos ambientales en las instalaciones de la empresa.

4. **Uso adecuado de activos:**
    - **Política**: Garantizar el uso adecuado de todos los activos de la empresa para mantener su integridad y disponibilidad.
    - **Procedimiento**: Establecer directrices claras para el manejo, uso y mantenimiento de todos los activos. Incluir políticas para el cuidado de dispositivos, procedimientos de acceso y manejo responsable de la información almacenada en los activos.
    - **Guia**: Instrucciones detalladas para el manejo adecuado de activos, incluyendo pautas sobre cómo utilizar, salvaguardar y mantener los activos. También, se proporcionan directrices para el acceso a la información y el uso responsable de los dispositivos y sistemas de la empresa.
5. **Transferencia de la información:**
    - **Política**: Establecer procesos seguros para la transferencia de datos entre sistemas y/o entidades externas.
    - **Procedimiento**: Definir protocolos seguros para la transferencia de información entre sistemas y partes externas. Incluir el uso de cifrado y autenticación, así como la verificación de la integridad de los datos durante el proceso de transferencia.
    - **Guia**: Instrucciones detalladas sobre cómo realizar la transferencia segura de datos. Incluye directrices para la configuración de conexiones seguras, la verificación de la autenticidad de los datos transferidos y el seguimiento de las transferencias para garantizar la integridad de la información.
6. **Dispositivos móviles:**
    - **Política**: Regular y salvaguardar el uso de dispositivos móviles para garantizar la seguridad de la información.
    - **Procedimiento**: Establecer lineamientos para el uso seguro de dispositivos móviles, incluyendo la implementación de contraseñas seguras, cifrado de datos, instalación de actualizaciones de seguridad y restricciones de acceso a redes no seguras.
    - **Guia**: Instrucciones detalladas sobre cómo configurar y mantener la seguridad en dispositivos móviles. Incluye pautas para el bloqueo remoto en caso de pérdida, uso de redes Wi-Fi seguras y buenas prácticas para proteger la información en dispositivos móviles.

7. **Restricciones en el uso/instalación del software:**
    - **Política**: Limitar la instalación y uso de software no autorizado para garantizar la seguridad y estabilidad de los sistemas.
    - **Procedimiento**: Establecer una lista de software aprobado y procedimientos para solicitar, revisar y autorizar la instalación de nuevos programas. Implementar controles para prevenir la instalación de software no autorizado.
    - **Guia**: Instrucciones detalladas sobre cómo solicitar y obtener la aprobación para instalar nuevo software. Incluye directrices para revisar y verificar la legitimidad de las aplicaciones, así como pasos para informar y manejar software no autorizado.
8. **Copias de respaldo:**
    - **Política**: Realizar copias de seguridad periódicas para garantizar la disponibilidad y recuperación de datos en caso de pérdida o daño.
    - **Procedimiento**: Programar y realizar copias de seguridad automáticas periódicas de todos los datos críticos. Verificar regularmente la integridad de las copias y almacenarlas en ubicaciones seguras fuera del sitio.
    - **Guia**: Instrucciones detalladas para configurar y supervisar copias de seguridad automáticas. Incluye pautas para verificar la integridad de los respaldos y procedimientos de recuperación en caso de pérdida de datos.
9. **Protección ante software malicioso:**
    - **Política**: Mantener soluciones de seguridad actualizadas para prevenir, detectar y mitigar software malicioso.
    - **Procedimiento**: Instalar y mantener software antivirus actualizado en todos los dispositivos. Realizar escaneos periódicos, configurar cortafuegos y aplicar parches de seguridad regularmente.
    - **Guia**: Instrucciones detalladas para la instalación y configuración de software antivirus. Incluye pautas para realizar análisis de virus, mantener actualizaciones de seguridad y procedimientos para identificar y manejar posibles infecciones.
10. **Gestión de vulnerabilidades:**
    - **Política**: Identificar, evaluar y mitigar vulnerabilidades en sistemas y aplicaciones para reducir el riesgo de explotación.
    - **Procedimiento**: Realizar análisis regulares de vulnerabilidades en sistemas, redes y aplicaciones. Clasificar, priorizar y abordar las vulnerabilidades identificadas siguiendo un plan de mitigación establecido.
    - **Guia**: Instrucciones detalladas sobre cómo llevar a cabo análisis de vulnerabilidades. Incluye directrices para la identificación, evaluación y resolución de vulnerabilidades, así como pasos para implementar parches y actualizaciones de seguridad.

11. Relaciones con los proveedores:

- **Política**: Establecer criterios de seguridad y confidencialidad para las relaciones con los proveedores.
- **Procedimiento**: Realizar evaluaciones de seguridad antes de la contratación, establecer acuerdos de confidencialidad y especificar requisitos de seguridad en los contratos. Gestionar regularmente las relaciones para asegurar el cumplimiento continuo de los estándares de seguridad.
- **Guia**: Instrucciones detalladas sobre cómo realizar evaluaciones de seguridad a proveedores, configurar acuerdos de confidencialidad y establecer requisitos de seguridad en contratos. Incluye directrices para la supervisión continua de la seguridad de los proveedores.

12. Gestión de incidentes de ciberseguridad:

- **Política**: Establecer un marco para la detección, respuesta y mitigación de incidentes de seguridad de la información.
- **Procedimiento**: Definir protocolos para la identificación, evaluación y respuesta a incidentes de seguridad. Designar roles y responsabilidades, establecer líneas de comunicación y procedimientos de escalada para manejar incidentes.
- **Guia**: Instrucciones detalladas sobre cómo identificar y reportar incidentes, roles y responsabilidades durante la respuesta a incidentes, y pasos a seguir para la recuperación y lecciones aprendidas después de un incidente.

13. Plan de continuidad del negocio:

- **Política**: Establecer directrices para mantener la operatividad y minimizar el impacto en caso de interrupciones significativas.
- **Procedimiento**: Identificar áreas críticas, evaluar riesgos, desarrollar estrategias de recuperación, implementar planes de contingencia y realizar pruebas periódicas para asegurar la efectividad del plan.
- **Guia**: Instrucciones detalladas para la activación del plan, incluyendo la notificación, activación de equipos, restauración de servicios críticos y procesos de comunicación con el personal y partes interesadas durante situaciones de crisis.

14. Formación y concienciación en ciberseguridad:

- **Política**: Establecer programas de formación continua para concienciar al personal sobre buenas prácticas y procedimientos de seguridad.
- **Procedimiento**: Desarrollar e implementar sesiones de formación periódicas, crear material educativo sobre seguridad cibernética y realizar pruebas de conocimientos para evaluar la comprensión.
- **Guia**: Instrucciones detalladas sobre cómo acceder y participar en programas de formación. Incluye directrices para el uso de material educativo, realización de pruebas y cómo reportar posibles incidentes de seguridad.

15. Seguridad en las operaciones:

- **Política**: Establecer directrices para garantizar la seguridad e integridad de las operaciones diarias de la empresa.
- **Procedimiento**: Definir y aplicar controles operativos para proteger sistemas, datos y procesos. Establecer procedimientos de control de cambios, monitorización y gestión de incidentes para garantizar la continuidad y seguridad operativa.
- **Guia**: Instrucciones detalladas sobre la implementación de controles operativos, incluyendo guías para el control de cambios, monitorización proactiva de amenazas y manejo de incidentes para preservar la seguridad y continuidad de las operaciones.