Política de Seguridad de Tecnología de la Información – Empresa XYZ

Departamento de seguridad de la información

1 de enero de 2024

**Contexto de la Organización**

La empresa XYZ es una organización de tamaño medio la cual se encarga de brindar servicios de transporte de personas, mercancías y valores, de capital netamente nacional. En su dirección cuenta con un personal administrativo y técnico calificado y con una estructura de mantenimiento, que permite mantener nuestros autobuses en condiciones óptimas para brindar un servicio eficiente y efectivo.

**Análisis de riesgos de la empresa XYZ**

Según el análisis del departamento de riesgos estos son los posibles riesgos que la empresa podría enfrentar:

* Violación de datos: Acceso no autorizado a sistemas que contienen información personal o financiera de clientes y empleados, lo que podría resultar en robo de identidad u otros tipos de fraude.
* Phishing e ingeniería social: Ataques de phishing y manipulación psicológica para obtener acceso a credenciales de inicio de sesión o información sensible.
* Ataques de malware y ransomware: Infección de sistemas con software malicioso que puede cifrar datos y exigir un rescate para su recuperación, lo que podría causar interrupciones operativas y pérdida de datos.
* Ataques de Denegación de Servicio (DDoS): Ataques que sobrecargan los sistemas con tráfico falso, dejando inoperables los servicios y afectando la experiencia del cliente.
* Fugas internas: Empleados maliciosos o descuidados que divulgan intencional o accidentalmente información confidencial de la empresa.
* Acceso no autorizado: Brechas en la gestión de accesos y permisos que permiten que personas no autorizadas accedan a sistemas y datos sensibles.
* Falta de encriptación: Datos almacenados o transmitidos sin cifrar, lo que podría exponer información sensible a posibles atacantes.
* Problemas de parchado: No aplicar parches de seguridad a tiempo, lo que puede dejar sistemas vulnerables a exploits conocidos.
* Inseguridad en aplicaciones web: Fallas en el desarrollo de aplicaciones web que podrían permitir a los atacantes acceder a información o comprometer sistemas.
* Falta de conciencia en seguridad: Falta de capacitación y conciencia entre los empleados sobre las prácticas de seguridad cibernética, lo que podría llevar a errores o malas decisiones.
* Dispositivos móviles no seguros: Uso de dispositivos móviles no seguros o no administrados para acceder a sistemas corporativos, lo que podría exponer datos sensibles.
* Copias de seguridad inadecuadas: Falta de copias de seguridad adecuadas de datos críticos, lo que podría hacer que la empresa pierda información importante en caso de un incidente.
* Fugas a través de terceros: Riesgo de que proveedores externos o socios comerciales no mantengan medidas de seguridad adecuadas y expongan los datos de la empresa.
* Uso de contraseñas débiles: Empleo de contraseñas débiles o reutilización de contraseñas, lo que podría facilitar el acceso no autorizado.
* Acceso físico no autorizado: Falta de medidas de seguridad física que permitan a personas no autorizadas acceder a equipos y sistemas.

**Política de Seguridad de Tecnología de la Información – Empresa XYZ**

**1. Introducción**

Esta Política de Seguridad de Tecnología de la Información establece las normas a seguir para proteger los activos de información y sistemas de tecnología de la información de la empresa XYZ. El objetivo es salvaguardar la confidencialidad, integridad y disponibilidad de la información, así como garantizar el cumplimiento de las leyes y regulaciones aplicables.

**2. Objetivos de Seguridad**

Los objetivos de esta política son:

* Proteger la confidencialidad: Asegurar que la información confidencial de la organización esté protegida contra accesos no autorizados.
* Salvaguardar la integridad de los datos: Garantizar que los datos almacenados y procesados en los sistemas de TI sean precisos, confiables y no estén sujetos a alteraciones no autorizadas.
* Garantizar la disponibilidad: Asegurar que los sistemas de TI estén disponibles y funcionen adecuadamente cuando sean requeridos, evitando interrupciones no planificadas.
* Fomentar la responsabilidad: Establecer roles y responsabilidades claros en cuanto a la seguridad de la información y las tecnologías utilizadas dentro de la organización.
* Cumplir con las leyes y regulaciones: Asegurarse de que la organización cumpla con todas las leyes y regulaciones aplicables relacionadas con la seguridad de la información y la privacidad de los datos.
* Mitigar riesgos de seguridad: Identificar y evaluar los riesgos de seguridad de TI y poner en marcha medidas para reducirlos y evitar posibles incidentes de seguridad.
* Sensibilizar sobre seguridad: Promover la conciencia de seguridad entre el personal, fomentando buenas prácticas y educándolos sobre las amenazas y cómo mitigarlas.

**Políticas de Seguridad de software**

A continuación, se presentan algunas de las políticas de seguridad que rigen el uso de la tecnología de la información dentro de la organización:

**1.1. Política de Contraseñas**

* Los usuarios deben crear contraseñas seguras que contengan una combinación de letras mayúsculas y minúsculas, números y caracteres especiales, mínimo 8 caracteres.
* Las contraseñas deben ser cambiadas cada 90 días y no deben ser compartidas con otras personas ni guardadas en lugares visibles.
* Se debe implementar la autenticación de dos factores para acceder a sistemas y servicios críticos y que contengan información sensible para la empresa.

**1.2. Política de Acceso y Privilegios**

* Se debe asignar a cada empleado el nivel de acceso necesario para llevar a cabo sus funciones laborales.
* Los privilegios de acceso deben ser revisados regularmente para garantizar que sean apropiados y actualizados según las responsabilidades del empleado.
* El acceso a información confidencial o sistemas críticos debe ser restringido y otorgado únicamente a empleados autorizados.
* Mientras el usuario s encuentre de vacaciones o cualquier periodo de descanso se inhabilitará el acceso a los sistemas de la empresa.

**1.3. Política de Respaldos y Recuperación de Datos**

* Se deben realizar copias de seguridad periódicas de los datos importantes y almacenarlas en ubicaciones seguras y fuera del sitio.
* Se debe realizar pruebas regulares de recuperación de datos para asegurar la efectividad del proceso de restauración.

**1.4. Política de Uso Aceptable**

* Los empleados deben utilizar los recursos de tecnología de la información de manera ética y legal.
* El acceso a Internet y el uso de correos electrónicos y redes sociales deben realizarse de manera responsable y en línea con los intereses de la organización. No se permite el uso de los dispositivos para uso personal.

**1.5. Política de Seguridad de Red**

* Se deben implementar firewalls, sistemas de detección de intrusiones y filtrado de contenido para proteger la red de amenazas externas.
* Las redes inalámbricas deben estar protegidas con cifrado y contraseñas seguras.

**1.6. Política de Manejo de Incidentes de Seguridad**

* Se debe establecer un procedimiento claro para reportar, gestionar y resolver incidentes de seguridad, incluyendo la notificación de violaciones de datos si es necesario.
* Se debe llevar a cabo una investigación adecuada de los incidentes de seguridad para determinar la causa y tomar medidas correctivas.

**2. Cumplimiento y Responsabilidad**

El cumplimiento de esta política es responsabilidad de todos los empleados y contratistas de la empresa XYZ. Cualquier violación de esta política puede resultar en acciones disciplinarias, incluida la terminación del empleo o acciones legales si corresponde.

**3. Revisión de la Política**

Esta política de seguridad de TI será revisada y actualizada periódicamente para reflejar los cambios en las amenazas de seguridad y la tecnología o las leyes aplicables.

**4. Disposiciones Finales**

Esta Política de Seguridad de Tecnología de la Información debe ser revisada y aceptada por todos los empleados, y se espera que todos los miembros del personal la cumplan en todo momento.

**Políticas de Seguridad de Hardware**

**1. Política de Resguardo de Equipos**

* Todos los equipos y dispositivos de TI deben estar físicamente protegidos contra el acceso no autorizado o el robo.
* Los equipos de escritorio y portátiles deben estar asegurados a mesas o escritorios con dispositivos de bloqueo (cable de seguridad) cuando sea necesario.
* Se debe implementar un procedimiento de registro y control para llevar un registro de los equipos y dispositivos asignados a cada empleado.

**2. Política de Actualización de Hardware**

* Los equipos y dispositivos de TI deben mantenerse actualizados con las últimas versiones de firmware y software de seguridad para mitigar vulnerabilidades conocidas.
* Se debe establecer un ciclo de vida para el hardware, y los equipos obsoletos deben ser retirados adecuadamente y eliminados siguiendo las regulaciones ambientales y de privacidad aplicables.

**3. Política de Acceso a Áreas Restringidas**

* El acceso a áreas físicas donde se encuentran los servidores y equipos críticos de TI debe estar restringido solo a personal autorizado.
* Los empleados deben usar credenciales de acceso, como tarjetas de identificación, para ingresar a áreas sensibles.

**4. Política de Mantenimiento de Hardware**

* Los equipos y dispositivos de TI deben ser revisados y mantenidos regularmente para asegurar su buen funcionamiento y durabilidad.
* Se deben realizar inspecciones periódicas para detectar y solucionar problemas de seguridad, como cables sueltos o dañados, ventilación obstruida, etc.

**5. Política de Desactivación y Disposición Segura**

* Antes de desechar cualquier equipo de TI, se debe realizar una limpieza adecuada para eliminar toda la información confidencial y datos del dispositivo.
* Los discos duros y medios de almacenamiento deben ser borrados o destruidos de manera segura antes de la disposición para evitar la recuperación de datos por parte de terceros no autorizados.

**6. Política de Uso de Dispositivos Extraíbles**

* Los empleados deben obtener autorización previa antes de conectar dispositivos extraíbles (como unidades USB, discos duros externos, etc.) a los sistemas de la organización.
* Los dispositivos extraíbles deben ser escaneados con antivirus antes de su uso en los sistemas de la empresa para prevenir la propagación de malware.

**7. Política de Administración de Contraseñas de BIOS y Firmware**

* Se debe establecer una contraseña segura para acceder a la BIOS y el firmware de los dispositivos, evitando cambios no autorizados en la configuración.
* El acceso y la administración de contraseñas de BIOS y firmware deben estar restringidos a personal de TI autorizado.

**8. Política de Seguridad de Dispositivos Móviles**

* Los dispositivos móviles propiedad de la organización deben estar protegidos con contraseñas o mecanismos de autenticación sólidos.
* Debe implementarse una solución de gestión de dispositivos móviles (MDM) para asegurar el control y la seguridad de los dispositivos móviles utilizados en la organización.

**9. Política de Actualización de Parches y Firmware**

* Los equipos de TI deben ser sometidos a un programa regular de actualización de firmware y aplicaciones para asegurar que se apliquen las últimas correcciones de seguridad.

**10. Política de Uso de Cámaras y Dispositivos de Grabación**

* El uso de cámaras y dispositivos de grabación debe estar sujeto a políticas y procedimientos específicos para proteger la privacidad de los empleados y los datos sensibles.

**11. Cumplimiento y Responsabilidad**

El cumplimiento de esta política es responsabilidad de todos los empleados y contratistas de la empresa XYZ. Cualquier violación de esta política puede resultar en acciones disciplinarias, incluida la terminación del empleo o acciones legales si corresponde.

**12. Revisión de la Política**

Esta política de seguridad de TI será revisada y actualizada periódicamente para reflejar los cambios en las amenazas de seguridad, la tecnología y las regulaciones aplicables.

**4. Disposiciones Finales**

Esta Política de Seguridad de Tecnología de la Información debe ser revisada y aceptada por todos los empleados, y se espera que todos los miembros del personal la cumplan en todo momento.

**Consideraciones Legales**

1. **Cumplimiento de Regulaciones**: La política de seguridad de TI cumplirá con todas las leyes y regulaciones aplicables en materia de protección de datos, privacidad, seguridad de la información y otros aspectos relacionados de acuerdo a las leyes de la Republica Dominicana como la ley 53-07 (sobre crímenes de alta tecnología), Ley No. 53-05 (sobre crímenes y delitos de alta tecnología), Ley No. 126-02 (sobre Comercio Electrónico, Documentos y Firmas Digitales) y cualquier otra ley aplicable.
2. **Privacidad de Datos Personales**: Garantizamos el cumplimiento de las leyes de protección de datos y privacidad al manejar y almacenar datos personales de empleados, clientes y terceros.
3. **Acceso y Monitoreo de Empleados**: Si la política incluye monitoreo o supervisión de las actividades de los empleados, los mismos serán informados.
4. **Consentimiento Informado**: Se informará a los empleados si se requiere el consentimiento de los empleados o usuarios para ciertas prácticas de seguridad, se obtendrá un consentimiento informado y claro de acuerdo con las leyes aplicables.
5. **Propiedad Intelectual y Derechos de Autor**: El uso de software, contenido y recursos de terceros debe cumplir con las licencias y derechos de autor correspondientes.
6. **Seguridad de la Información en Contratos**: Los contratos con proveedores de servicios de TI o terceros incluirán cláusulas de seguridad y protección de datos.
7. **Notificación de Violaciones de Datos**: Si se produce una violación de datos, se deberá notificar a las partes afectadas y a las autoridades correspondientes según lo requiera la ley.

**Consideraciones Éticas**

1. **Transparencia y Consentimiento**: La organización se compromete a ser transparente con los empleados y usuarios sobre las prácticas de seguridad y obtener su consentimiento informado cuando sea necesario.
2. **Equidad y No Discriminación**: Se aplicará de manera justa y sin discriminación a ningún grupo de empleados o usuarios.
3. **Confidencialidad y Confianza**: Se respetará la confidencialidad de la información de los empleados y usuarios.

**Alcance**

La presente Política de Seguridad de la Información se crea en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de empresa XYZ. En particular, debe ser conocida y cumplida por todo el personal vigente de la empresa sin importar su función.

**Plan de implementación**

**Objetivo del Plan:** Implementar la Política de Seguridad de Tecnología de la Información en la institución para proteger los activos de información y sistemas de TI, garantizar el cumplimiento de las leyes y regulaciones, y promover una cultura de seguridad entre los empleados.

**Duración del Plan:** El plan de implementación se llevará a cabo en un período de seis meses.

**Recursos Necesarios:**

* Equipo de Proyecto de Seguridad de TI: Liderado por un gerente de seguridad de TI y compuesto por representantes de los departamentos clave, como TI, recursos humanos y operaciones.
* Presupuesto para Capacitación: Se destinará un presupuesto para brindar capacitación en seguridad de TI a todos los empleados.
* Herramientas y Software de Seguridad: Adquisición de herramientas y software de seguridad necesarios para aplicar las políticas.

**Fase 1: Planificación y Diseño (Mes 1)**

1. Formación del Equipo de Proyecto de Seguridad de TI:
   * Identificar a los miembros del equipo y asignar responsabilidades específicas.
   * Designar un líder del equipo encargado de supervisar el proceso de implementación.
2. Evaluación de Riesgos:
   * Realizar una evaluación de riesgos de TI para identificar posibles vulnerabilidades y amenazas.
   * Priorizar los riesgos y determinar las áreas que requieren una atención inmediata.
3. Adaptación de la Política de Seguridad:
   * Personalizar la Política de Seguridad de TI de acuerdo con las necesidades y estructura de [nombre de la organización].
   * Asegurar que las políticas sean claras y comprensibles para todos los empleados.
4. Presupuesto y Adquisiciones:
   * Establecer un presupuesto para la implementación de la política, incluyendo la compra de herramientas y software de seguridad necesarios.
5. Capacitación del Personal:
   * Planificar sesiones de capacitación en seguridad de TI para todos los empleados.
   * Diseñar materiales de capacitación, incluidas presentaciones y material escrito.

**Fase 2: Implementación (Meses 2-4)**

1. Comunicación y Concientización:
   * Comunicar a todos los empleados la nueva Política de Seguridad de TI y su importancia.
   * Lanzar campañas de concientización para destacar las principales prácticas de seguridad y la forma en que afectan a la organización.
2. Implementación de Políticas Específicas:
   * Implementar las políticas específicas, como la Política de Contraseñas, Política de Acceso y Privilegios, Política de Seguridad de Red, etc.
   * Garantizar que los controles de seguridad se apliquen de manera coherente en toda la organización.
3. Actualización de Sistemas y Software:
   * Realizar actualizaciones de seguridad en todos los sistemas y software para proteger contra vulnerabilidades conocidas.
4. Configuración de Seguridad:
   * Configurar firewalls, sistemas de detección de intrusiones y otros mecanismos de seguridad según lo definido en la política.
5. Implementación de MDM y Seguridad de Dispositivos Móviles:
   * Configurar y desplegar una solución de gestión de dispositivos móviles (MDM) para proteger y controlar los dispositivos móviles utilizados en la organización.

**Fase 3: Monitoreo y Evaluación (Meses 5-6)**

1. Auditoría y Evaluación de la Política:
   * Realizar una auditoría para evaluar el cumplimiento de la Política de Seguridad de TI en todos los departamentos.
   * Identificar áreas de mejora y posibles brechas de seguridad.
2. Evaluación Continua de Riesgos:
   * Continuar con la evaluación periódica de riesgos de TI para identificar nuevas amenazas y vulnerabilidades.
3. Reporte de Incidentes y Manejo de Incidentes:
   * Establecer un sistema para reportar y manejar incidentes de seguridad de manera efectiva.
4. Capacitación Continua:
   * Proporcionar capacitación continua en seguridad de TI para mantener a los empleados actualizados con las últimas amenazas y mejores prácticas.
5. Mejora Continua:
   * Ajustar y mejorar la Política de Seguridad de TI según las lecciones aprendidas y los cambios en el entorno de seguridad.