política de seguridad digital y de seguridad de la información

seguridad de la información mencionadas:

1. **Política de acceso y control de información:**
    - **Objetivo:** Garantizar que solo el personal autorizado tenga acceso a los sistemas y datos de la organización, protegiendo así la confidencialidad e integridad de la información.
    - **Procedimiento:** Todo acceso a los sistemas de información de la organización debe requerir autenticación mediante credenciales únicas para cada usuario. Se utilizarán controles de acceso basados en roles para limitar los privilegios de acceso a la información según las necesidades laborales de cada usuario. Se implementarán medidas de control de acceso físico y lógico para proteger los recursos de información contra accesos no autorizados.
2. **Política de seguridad de contraseñas:**
    - **Objetivo:** Garantizar contraseñas seguras y su gestión adecuada para proteger los sistemas y datos de la organización contra accesos no autorizados.
    - **Requisitos:**
        - Las contraseñas deben tener al menos 12 caracteres de longitud.
        - Deben incluir una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.
        - Las contraseñas no deben basarse en información personal fácilmente identificable.
        - Se requiere el cambio de contraseña al menos cada 90 días.
    - **Prohibiciones:**
        - No se permiten contraseñas compartidas.
        - No se permite el uso de contraseñas anteriores.
        - No se permiten contraseñas almacenadas en texto plano.
3. **Política de uso aceptable de recursos informáticos:**
    - **Objetivo:** Establecer normas y restricciones para el uso adecuado de los recursos informáticos de la organización.
    - **Procedimiento:** Los empleados deben utilizar los recursos informáticos de la organización de manera responsable y ética, evitando actividades como el acceso a contenido inapropiado, la descarga de software no autorizado y el uso indebido de la red corporativa para actividades personales.

4. **Política de seguridad de la red:**
    - **Objetivo:** Proteger la red de la organización contra amenazas como malware, intrusiones y ataques de denegación de servicio.
    - **Medidas de seguridad:** Implementar firewalls, sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS) para monitorear y proteger la red contra actividades maliciosas. Aplicar cifrado para proteger la comunicación sensible a través de la red.
5. **Política de gestión de parches:**
    - **Objetivo:** Mantener actualizados los sistemas y aplicaciones con los últimos parches de seguridad para protegerlos contra vulnerabilidades conocidas.
    - **Procedimiento:** Establecer un proceso para identificar, descargar, probar e implementar parches de seguridad en todos los sistemas y aplicaciones de la organización de manera oportuna y eficiente.
6. **Política de respaldo y recuperación de datos:**
    - **Objetivo:** Garantizar la disponibilidad y la integridad de los datos críticos de la organización mediante la realización periódica de copias de seguridad y la implementación de medidas de recuperación en caso de pérdida o corrupción de datos.
    - **Procedimiento:** Realizar copias de seguridad periódicas de los datos críticos de la organización y almacenarlas de forma segura en ubicaciones externas. Probar regularmente los procedimientos de recuperación de datos para garantizar su eficacia.
7. **Política de gestión de incidentes de seguridad:**
    - **Objetivo:** Establecer un proceso para detectar, investigar y responder a incidentes de seguridad cibernética con el fin de minimizar el impacto en la organización y proteger la información crítica.
    - **Procedimiento:** Todo incidente de seguridad debe ser reportado al equipo de seguridad de la información de manera inmediata. Se debe realizar una evaluación inicial para determinar la naturaleza y el alcance del incidente. Se implementarán medidas correctivas para mitigar el incidente y prevenir futuros ataques. Se documentará el incidente, incluyendo las acciones tomadas y lecciones aprendidas, para mejorar los procesos de seguridad futuros.

8. **Política de privacidad de la información:**
    - **Objetivo:** Proteger la privacidad y confidencialidad de la información personal de los empleados y clientes de la organización.
    - **Requisitos:** Establecer controles para garantizar que la información personal se recopile, almacene, utilice y comparta de manera legal y ética. Informar a los empleados y clientes sobre cómo se utiliza y protege su información personal.
9. **Política de educación y concienciación en seguridad:**
    - **Objetivo:** Mejorar la conciencia y la competencia de los empleados en materia de seguridad cibernética y protección de la información.
    - **Actividades:** Proporcionar formación periódica sobre prácticas seguras en el uso de la tecnología y la protección de la información. Realizar simulacros de phishing y otros ejercicios de concienciación en seguridad.
10. **Política de cumplimiento normativo:**
    - **Objetivo:** Garantizar que la organización cumpla con todas las leyes y regulaciones aplicables en materia de seguridad de la información.
    - **Requisitos:** Realizar evaluaciones periódicas de cumplimiento para identificar y abordar posibles brechas de seguridad. Mantener registros de cumplimiento y cooperar con las autoridades reguladoras en caso de investigaciones o auditorías.