POLICIES PROJECT

Proyecto de Políticas de compañia para curso Coursera
Juan Felipe **Rodriguez Galindo**

EVALUACIÓN

El objetivo de esta tarea es ayudarlo a comprender que no todas las políticas organizacionales son iguales. Escribirás tu propia política de seguridad para una empresa mediana basada en otras políticas organizativas que se han escrito en la industria.

CRITERIOS DE REVISIÓN

La tarea se calificará según la **rigurosidad de la política y la investigación de apoyo** realizada.

ANTECEDENTES E INSTRUCCIONES

ANTECEDENTES:

En la lección 2, discutimos la necesidad de políticas organizacionales. La mayoría de las políticas organizacionales son diferentes de alguna manera, pero pueden contener muchas de las mismas características. Las políticas están destinadas a ser seguidas y, por lo general, no contienen mucha información innecesaria o reglas a seguir. La información contenida en la política generalmente proviene de algo que sucedió en el pasado.

En esta tarea, deberá realizar una investigación sobre cómo se ven las políticas organizacionales, discutir cómo son iguales o diferentes. Luego, elegirá uno de los suyos para escribir basándose en algo que sepa.

Por ejemplo, me encanta jugar videojuegos, así que buscaré el sitio web de algunos minoristas de videojuegos y veré sus políticas. Luego los compararé y los discutiré.

Luego, tomaré el mismo concepto, mi minorista de videojuegos, y diseñaré mi propia política basada en una de las políticas de ejemplo en la sección de ejemplos de la lección 2 escrita por SANS.

PASOS:

- Repaso de la lección 2
- Elija de 3 a 4 empresas u organizaciones para revisar sus políticas
- Analice en qué se diferencian las políticas entre sí y discuta en qué se parecen.
- Además, brinde su propia perspectiva sobre cómo las políticas podrían afectar como consumidor.
- Elija una política de ejemplo de SANS y cree la suya propia para la industria u organización que le interesa.
- Reflexione sobre la experiencia y cómo abordó el problema.

SU MISIÓN:

Envíe sus respuestas en los cuadros de texto a continuación.

- **Elija de 3 a 4 empresas** u organizaciones para revisar sus políticas. ¿**En qué se diferencian y cómo podrían ser iguales**? Envíe los **nombres de las empresas** y las **políticas que revisó**.
- Elija una **política de ejemplo de SANS** y **cree la suya propia** para la industria u organización que le interesa.
- **Reflexiona sobre la experiencia** y **cómo abordaste el problema**.

DESARROLLO PROYECTO

1. **Politicas revisadas:** Politicas para la creacion de contraseñas.

   Empresas Revisadas: Microsoft, IBM, Weill cornell medicine, University of georgia, Universidad de Sevilla.

   Diferencias y Similitudes: En primer lugar las **Diferencias** las cuales radican principalmente en la extensión de las políticas y el campo que abarcan cada una de ellas, es decir, por ejemplo en las políticas que maneja windows 10 que son básicamente las mismas que outlook vemos que no hay una relevancia de cómo la compañía maneja la seguridad de las contraseñas dadas por el usuario. Otra gran diferencia es el hecho de que algunas empresas cierran el paso de exportar las contraseñas fuera de la organización, esas son las que más recalco o que tienen una mayor influencia para el curso ya que estas tienen un peso muy alto en lo desarrollado en el curso.

   Ahora para enunciar algunas **Similitudes** también muy importantes podemos ver que cada empresa utiliza de forma integra una serie de lineamientos para mejorar la seguridad de las contraseñas, por ejemplo la longitud, la cantidad de números que debe contener, entre otras.

   Para realizar la comparativa aunque revise diversas fuentes tomé como políticas principales para el ejercicio las de la **Universidad de Sevilla**, la **Universidad de Georgia** y la empresa **Weill Cornell Medicine Information Technologies & Services**, ya que para mi fueron las que más resaltan dentro del campo de políticas, ya que tenia muchas diferencias y punto de vista muy diferentes unas de otras.

   En cuanto a estas podemos denotar las **similitudes** de que las tres no permiten la salida de las contraseñas fuera de la institución y que todas estas no son transferibles ni siquiera dentro de las organizaciones, otra característica similar es que estas tienen una guía para la construcción con el fin de ser seguras en la institución.

   Ahora hablando de las **diferencias** podemos hablar de la universidad de Georgia la cual establece un apartado de políticas diferentes o complementarias para los administradores y los desarrolladores del sistema, por otro lado la diferencia más notable se da en las políticas de Weill Cornell Medicine ya que son las más robustas de estas tres ya que posee varios apartados con el fin de cubrir todas las situaciones posibles que se puedan dar, por ejemplo cuando se bloquea la cuenta, las responsabilidades que

debe tener el sistema, las responsabilidades del usuario con la contraseña, entre otras.

2. Directrices para la construcción de contraseñas aplicadas a medianas empresas en Colombia.

Resumen. Las contraseñas son un componente crítico de la seguridad de la información. Las contraseñas sirven para proteger las cuentas de los usuarios; sin embargo, una contraseña mal construida puede resultar en el compromiso de sistemas, datos o redes individuales . Esta guía proporciona las mejores prácticas para crear contraseñas seguras,aplicadas al sector de pequeñas y medianas empresas dentro del sector productivo colombiano.

Propósito. El propósito principal de estas pautas es proporcionar una guía para mejorar las prácticas actuales para la creación de contraseñas seguras, dentro de pequeñas y medianas empresas en Colombia.

Alcance. Esta directriz se aplica a los empleados, contratistas, consultores , trabajadores temporales y de otro tipo , incluido todo el personal afiliado a terceros. Esta guía se aplica a todas las contraseñas, incluidas, entre otras, las cuentas de nivel de usuario, cuentas de nivel de sistema, cuentas web, cuentas de correo electrónico, protección de protector de pantalla, correo de voz e inicios de sesión de enrutador local.

Objetivos. Establecer las políticas o buenas prácticas en el uso de un sistema de gestión de contraseñas para el control de accesos.

Declaración de directrices. Los principales puntos de la política que se plantea son:

- Gestión de la contraseña. La gestión de contraseñas en el mundo de las tecnologías de la información es uno de los aspectos más delicados para asegurar el acceso a sus sistemas. en síntesis se ocupa de:
    - Identificar los equipos, servicios y aplicativos a los que se necesitan acceder.
    - Definir cómo se generan las claves predeterminadas, así como su formato.
    - Distribución de las claves generadas (Definir método y cifrado, como se activan las claves).
    - Almacenamiento de claves, repositorios seguros y copias de respaldo.
    - Determinar de forma clara cómo y quién tiene acceso con el fin de poder realizar una debida auditoría del sistema.

    - Establecer periodos en los que son seguras las contraseñas con el fin de volver la seguridad de un proceso cíclico y que cambie continuamente con el fin de reforzar la seguridad.
    - Determinar los procesos de revocación de accesos por parte del sistema cuando un usuario sea dado de baja en la organización
    - Las contraseñas deben ser robustas, para crear una contraseña segura seguiremos una serie de lineamientos para poder realizar la correcta robustez de la contraseña el cual estará al final de esta sección.
- Técnicas de autenticación externas, en el caso de una pequeña empresa no se ve necesario el uso de esta metodología para realizar el ingreso aunque siempre puede existir la posibilidad de que se maneje, por lo cual también cubriremos la posibilidad de implantación.
    - En este punto después de revisar con detenimiento las diferentes técnicas que se pueden utilizar, se evidencia que para pequeñas o medianas empresas la mejor forma de autenticación si se requiere usar estas formas será el social-login, el cual con alternativas como google y microsoft que tienen servidores muy seguros para realizar un proceso de autenticación confiable.
- No se debe utilizar las contraseñas generadas por el sistema, para esto debemos realizar un cambio inmediatos en el primer login en el sistema.
- Cambio de contraseña de forma periódica, con el fin de volver más difícil el uso de técnicas de penetración al sistema en el que estamos.
- Tener en cuenta el uso de un generador de contraseñas ya que si se usa uno muy simple puede ser muy fácil de descifrar.
- Creación de metadatos para la generación de contraseñas con el fin que guarde el motivo por el que crea una clave, la fecha y otros datos de vital importancia de los cuales se pueda extraer información en caso de una auditoría por parte del administrador del sistema.
- Tratar de no utilizar la misma contraseña fuera de empresa o con otros servicios con el fin de no extender las vulnerabilidades de la contraseña a otro sistema.
- Uso del doble factor en la autenticación para el ingreso del sistema (ya sea a otro correo seguro o con una clave biométrica).
- No compartir la contraseña o con nadie fuera de la empresa (ni ponerlas en físico en papeles o libretas que esten a la merced de otras personas en la organización)
- Es vital no hacer uso de la herramienta que tienen algunos dispositivos o navegadores para recordar las contraseñas, ya que estas pueden ser una gran vulnerabilidad si el dispositivo sale de la empresa.

Checklist o cumplimiento de políticas. Checklist con el fin de verificar que las directrices se cumplan.

Estándares, políticas y procesos relacionados.
Política de contraseñas de la Universidad de Sevilla.

Referencias.
https://blog.devolutions.net/2018/02/top-10-password-policies-and-best-practices-for-system-administrators

ANEXO

Para que la contraseña sea robusta se recomienda que las contraseñas

- Deben estar compuestas de por lo menos ocho caracteres;
- Esta debe combinar caracteres de distinto tipo (minúsculas, mayúsculas , símbolos y números);
- Las contraseñas no deben contener los siguientes tipos de palabras:
    - palabras simples en cualquier idioma (palabras de diccionarios no son recomendables);
    - nombres propios, fechas, lugares o datos de carácter personal;
    - palabras que estén formadas por caracteres próximos en el teclado (ej. 123456);
    - palabras excesivamente cortas.
- Se evitará el uso de claves formadas por elementos o palabras que puedan ser públicas o muy simples para adivinar (ej. nombre + fecha de nacimiento);
- Se establecerán contraseñas más fuertes para el acceso a aquellos servicios o aplicaciones más críticas, llevando aplicaciones con autenticación de doble factor;
- Se tendrá en cuenta lo expuesto en los puntos anteriores también en el caso de utilizar contraseñas de tipo passphrase(contraseña larga formada por una secuencia de palabras)

3. **Experiencia ->**

La creacion de estas políticas a mi parecer son bastante complejas y requieren en gran medida de un arduo trabajo en el proceso inicial de elaboración, aunque contamos con herramientas como las que nos proporciona SANS gran parte de este proceso también debe ser acomodado o personalizado según las necesidades de la empresa en la que trabajamos. También que para cada caso de uso se podría también crear políticas específicas que otorguen a un administrador de sistemas una opción más viable para auditar o manejar un sistema, esto buscando la eficiencia y procesos más óptimos.

También para la creación o estipulación de estas lo preferible también es tomar como base una metodología de desarrollo en espiral para el manejo y el constante mejoramiento de estas políticas, se puede comparar este

proceso como el de realizar ciertas actualizaciones a nuestras políticas de forma constante e iterativa.

Cómo abordaste el problema->

En primer lugar la elección de una política, la elección de una política para mí fue una sección fundamental durante el desarrollo de un trabajo realizado de forma cómoda y preservando una calidad alta. Por esto elegí como eje principal el uso y creación de contraseñas dentro de un sistema, ya que el tema normalmente suele ser obviado por las personas que interactúan con los sistemas utilizando claves débiles.

En segundo lugar la elección de las fuentes de donde realizaremos la recolección de información para desarrollar nuestras propias políticas, también un paso fundamental ya que en cuanto podamos seguir o revisar un modelo ya probado y bien documentado podemos nosotros realizar el proceso de estipulación de reglas al momento de elegir o generar una contraseña.

Ya para finalizar una revisión completa, es decir, evaluar personalmente el modelo y llevarlo luego a comparación con otros modelos de políticas utilizados dentro de la industria de las tecnologías de la información, con el fin de detectar posibles fallos y agregarle cierta robustez a las políticas generadas.

REFERENCIAS

- https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy
- https://www.ibm.com/support/knowledgecenter/en/ssw_aix_72/security/aix_sec_expert_pwd_policy_settings.html
- https://its.weill.cornell.edu/policies/1115-password-policy-and-guidelines
- https://eits.uga.edu/access_and_security/infosec/pols_regs/policies/passwords/password_standard/
- https://blog.devolutions.net/2018/02/top-10-password-policies-and-best-practices-for-system-administrators
- https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blta5be14c7136a535f/5e9dde89db124263e8afce3d/password_construction_guidelines.pdf
- https://sic.us.es/sites/default/files/seguridad/politica_de_contrasennas_us.pdf
- https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas.pdf
- https://docs.microsoft.com/en-us/azure/active-directory/develop/
- Echeverry, A. M. L., & Sánchez, P. A. V. (2016). Política de gestión de contraseñas para usuarios finales. *Scientia et technica*, *21*(2), 128-134.