SEGURIDAD INFORMÁTICA DE LOS SISTEMAS DE INFORMACIÓN

Las políticas de seguridad informática tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos)) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de las empresas.

Las políticas de seguridad dispuestas en este documento son aplicables a todos los empleados, contratistas, consultores, eventuales y otros empleados de la empresa.

El objetivo de las políticas de seguridad presentes en este documento es guiar los procesos relacionados

- Control de acceso (aplicaciones, base de datos,etc)
- Resguardo de la Información
- Gestión de la continuidad del negocio
- Protección contra intrusión
- Monitoreo de la seguridad
- Identificación y autenticación
- Utilización de recursos de seguridad
- Privacidad

POLÍTICAS DE SEGURIDAD FÍSICA

Acceso físico

Los sistemas de información se encontrarán alojados en servidores virtuales (nube) pertenecientes a la empresa Amazon Web Service (**AWS**), por lo tanto la seguridad física de los mismos será responsabilidad de dicha empresa.

Respaldos

Las bases de datos de la empresa serán respaldadas **diariamente** en forma manual y/o automática.

Los respaldos deben almacenarse en servidores de contingencia y equipos distintos a donde se aloja la base de datos original permitiendo tener contingencia y continuidad de negocio.

Para reforzar la seguridad de la información, los usuarios, bajo su criterio, deberán

hacer respaldos de la información en sus discos duros frecuentemente, dependiendo de la importancia y frecuencia de cambio; y en las unidades de almacenamiento asignadas por la empresa en “La Nube” (Google Drive), deberá realizar una sincronización continua de la información importante de la empresa.

Los recursos digitales de la empresa serán respaldados **mensualmente** o después de eventos de carga masiva de recursos digitales (catalogación de un programa académico).

Los respaldos deben almacenarse en un espacio físico diferente al original, conservando sólo la última sincronización realizada y un respaldo de eliminados de la misma que se almacenará solo por una sincronización.

POLÍTICAS DE SEGURIDAD LÓGICA

Servidores

Los administradores de tecnología de información (**ATI**) son responsables de la configuración de todo servidor que pertenezca o provea un sistema de información para la empresa.

Dentro de la configuración de los servidores deben tenerse en cuenta los siguientes componentes de seguridad:

- Debido a que los servidores se alojan en sistemas remotos el acceso a estos debe ser realizado a través del protocolo **ssh**, y solo puede ser accedido por conexiones que provengan de direcciones **IP** autorizadas por este documento.
- **AWS** (proveedor de servicio web) utiliza la criptografía de clave pública para cifrar y descifrar la información de inicio de sesión (**Key Pair**). Para realizar la conexión vía ssh al servidor se requiere esta **Key.** Esta llave debe ser reemplazada cada **tres (3) meses**.
- Durante la configuración de los servidores deben generarse las normas para el uso de los recursos del sistema, principalmente la restricción de directorios, permisos y programas a ser ejecutados.
    - Para ello deben generarse usuarios específicos para las tareas que les corresponda realizar al interior de los servidores. Algunas de las categorías que deben tenerse en cuenta son: Administrador de Bases de datos, Soporte y mantenimiento, Administrador de repositorios.
    - Todo usuario con acceso a los servidores debe poseer una contraseña segura (**Ver apartado de contraseña segura**).
    - Estas contraseñas deben ser modificadas cada **tres (3) meses** siguiendo siempre el patrón de contraseñas seguras.

- Los servidores que proporcionen servicios deberán recibir un mantenimiento periódico por parte de los ATI para garantizar su correcto funcionamiento. Dicho mantenimiento debe realizarse siguiendo las siguientes características:
    - Mantenimiento **semestral** donde se realice depuración de logs
    - Mantenimiento **anual** que incluya la revisión de configuración de software
- Los servidores deben permanecer en constante monitoreo por parte de los ATI. Dicho proceso debe realizarse de forma manual o automática.

Bases de datos

Los **ATI** son responsables de la configuración y mantenimiento de todas las bases de datos relacionadas al negocio.

Dentro de la configuración de las bases de datos deben tenerse en cuenta los siguientes componentes de seguridad:

- El acceso a los sistemas de información, deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información de la empresa.
    - Para ello deben generarse usuarios específicos para las tareas que les corresponda realizar al interior de la base de datos. Algunas de las categorías que deben tenerse en cuenta son: administradores, usuarios de ejecución, usuarios de consulta y usuarios de gestión.
    - Todo usuario con acceso a la base de datos debe poseer una contraseña segura (**Ver apartado de contraseña segura**).
    - Estas contraseñas deben ser modificadas cada **tres (3) meses** siguiendo siempre el patrón de contraseñas seguras.
- El administrador de la base de datos es el **ÚNICO** encargado de asignar las cuentas a los usuarios para el uso.
- Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes

Direcciones IP válidas

- Red interna de la oficina calle 72

Contraseña segura

Una contraseña segura es una que no puede ser fácilmente determinada por otro usuario ya sea que la adivine o que utilice programas automáticos.

Algunos aspectos que debe tener son:

- Utilizar combinación de letras mayusculas y minusculas
- Utilizar combinaciones alfanuméricas
- Incluir caracteres especiales como: - * ? ! @ # $ / () {} = . , ; :
- No debe tener espacios en blanco
- Debe tener una longitud mayor o igual a 16 caracteres.

Otros aspectos a tener en cuenta pero esta vez para ser evitados:

- No se debe utilizar información personal ni tampoco relacionada al elemento que estemos protegiendo.
- No se deben utilizar patrones secuenciales (1234) ni comunes (qwerty)
- No se recomienda repetir caracteres (1111111).
- No comunique la contraseña con nadie.
- Nunca anote la contraseña en un papel para recordarla
- No incluya nunca su contraseña en programas de mensajería, correo electrónico, ni otros dominios diferentes a **@kuepa.com**

PROTOCOLO DE RESTABLECIMIENTO

Generalidades

1. Crear y lanzar instancia en AWS que corresponda al servidor requerido.
2. Montar imagen base con software necesario para funcionar.
3. Si se requiere incluir la instancia en el balanceador de carga.

Específico

1. Servidor Web
    a. Importar la(s) base(s) de datos que se requieran.
    b. Lanzar script de aplicativo específico que desea configurar:
        - Reemplaza los archivos de configuración de apache (virtual host, hosts).
        - Descargar el código de la aplicación.
        - Configurar y lanzar aplicaciones en tiempo real (NodeJS) si se requieren
        - Configurar aplicación según corresponda (Conexión BD, Archivos de caché, archivos de log, carpetas de imágenes, Estructura de carpetas según corresponda)

c. Importar recursos digitales (imágenes, videos, audios, etc) según corresponda.

2. Servidor Base de datos
   a. Importar la(s) base(s) de datos que se requieran.
   b. Lanzar script de creación de usuarios de las bases de datos.
   c. Lanzar script de actualización de datos de conexión de las aplicaciones relacionadas a la BD que se está configurando.

Acción	Tipo	Aplica sobre	Tiempo*	Recursos
1	General	AWS	30m	Imagen instancia
3	General	AWS	10m	Instancia AWS generada
1 - a	Específico	Serv. Web	2h 30m	Conexión SSH, Backup de BD, Conexión estable a internet y ancho de banda amplio
1 - b	Específico	Serv. Web	30m	Script de la aplicación a configurar, Conexión a SSH, Conexión estable a internet y ancho de banda amplio
1 - c	Específico	Serv. Web	2h	Backup de recursos digitales, Conexión FTP, Conexión a SSH, Conexión estable a internet y ancho de banda amplio
2 - a	Específico	Serv. BD	2h 30m	Conexión SSH, Backup de BD, Conexión estable a internet y ancho de banda amplio
2 - b	Específico	Serv. BD	30m	Script de creación de usuarios de BD, Conexión a SSH, Conexión estable a internet y ancho de banda amplio
2 - c	Específico	Serv. BD	30m	Script actualización de la aplicación a configurar, Conexión a SSH, Conexión estable a internet y ancho de banda amplio

* Los tiempos están sujetos a variación por el estado de conexión a internet y de acuerdo a la aplicación que se esté configurando.

ASIGNACIÓN DE PERMISOS PARA USUARIOS DE BASES DE DATOS

A continuación se relacionan las políticas a tener en cuenta a la hora de crear usuarios de MYSQL ya sea de aplicaciones propias o para terceros según corresponda, se detalla el énfasis que debe tener cada tipo de usuario según las acciones que debe desempeñar, se van a dividir entre aspectos generales y específicos para tipos de usuarios.

Aspectos generales:

Estos aspectos se encaminan a la forma en que se deben generar los usuarios para la interacciones entre aplicaciones y de ellas mismas, con el fin de que si se necesita realizar algún tipo de control se fácil identificar desde donde se están realizando las peticiones y poder analizar comportamientos, a continuación se listan los aspectos:

- **Usuario por aplicación:** Cada aplicación que conforme el ecosistema tecnológico de kuepa o de cualquier tercero que intervenga debe tener un usuario único que haga referencia a la aplicación desde la que se ejecuta.

- **Usuarios entre aplicaciones:** De existir la necesidad de que un usuario se conecte a la base de datos de otra aplicación, se debe crear un usuario donde se indique la procedencia y el destino para identificar esta interacción fácilmente.

- **Usuarios para operaciones externas:** Para generar backups o cambios importantes sobre los esquemas se debe determinar un usuario con los permisos necesarios y que se use específicamente para estas acciones.

- **Nombrado de usuarios:** Los nombres deben tener mayúsculas y minúsculas, números y caracteres del alfabeto inglés con el fin de mejorar la seguridad de los sistemas.

- **Permisos pertinentes:** Los usuarios deben contar con los permisos que requiera para su operación, se debe evitar garantizar todos los permisos a diferentes usuarios, los permisos que se asignen a un usuario solo deben afectar al schema que se desea manipular con este usuario.

- **Revisión periódica:** Se recomienda realizar una revisión periódica de los usuarios y sus privilegios con el fin de validar que los mismos y que se mantengan como se dejaron la última vez.

Aspectos específicos:

Estos aspectos se encaminan a la distinción entre diferentes tipos de usuario que puedan interactuar en algún momento con los schemas de MYSQL, como lo son, los usuarios administradores, usuarios de ejecución, usuarios de consulta y usuarios de gestión.

El motor de bases de datos MYSQL ofrece bastantes y diferentes tipos de permisos que pueden ser agregados a los usuarios, cada uno de estos enfocado a diferentes acciones que se pueden realizar dentro del motor, en la imagen 1 se listan los diferentes permisos y los contextos en que aplican.