## Marco de Cyberseguridad:

### Identificar (ID):

La función Identificar está vinculada a la comprensión del contexto de la organización, de los activos que soportan los procesos críticos de las operaciones y los riesgos asociados pertinentes. Esta comprensión permite definir los recursos y las inversiones de acuerdo con la estrategia de gestión de riesgos y sus objetivos.

Las categorías dentro de esta función son: Gestión de activos; Ambiente del negocio; Gobernanza; Evaluación de riesgos y Estrategia para la gestión de riesgos.

##### En nuestro proyecto la parte de identificar seria:

Los activos son:

1- Servidores

2- Equipos(PC) del registro de la entrada

3- Equipos(PC) de la parte de administración de la utu

4- Switch

5- LAN

Vulnerabilidades:

1- Robo de Equipos(PC)

2- Fallos en el equipo y servidor

3- Robo de información desde el servidor

4- Corte de luz

5- Incendios

6- Inundación

Control de Seguridad:

1- Equipo de respaldo

2- El personal que esté autorizado tiene acceso al centro de datos

3- Centro de respaldo de datos que está asegurado

4- Disco duros cifrados

### Proteger (PR):

Es una función vinculada a la aplicación de medidas para proteger los procesos y los activos de la organización, independientemente de su naturaleza TI.

Las categorías dentro de esta función son: Control de acceso; Concientización y formación; Seguridad de los datos; Procesos y procedimientos para la protección de la información; Mantenimiento y Tecnología de protección.

##### En nuestro proyecto la parte de identificar seria:

Objetivo General de Seguridad:Garantizar la integridad, confidencialidad y disponibilidad del sistema de gestión de entrada a la institución, al tiempo que se abordan las vulnerabilidades identificadas.

1. Protección de Datos y Acceso:

- Implementar autenticación segura para los usuarios que acceden al sistema.

- Utilizar cifrado para proteger los datos de los usuarios, como información personal y registros de entrada.

2. Protección Física:

- Implementar controles de acceso físico a las instalaciones de la institución, donde se ubica el sistema.

- Proteger los equipos y servidores del sistema contra robos.

3. Disponibilidad del Sistema:

- Implementar redundancia en servidores y equipos críticos para garantizar la disponibilidad.

- Establecer un plan de continuidad de negocios para gestionar situaciones de interrupción del servicio, como cortes de energía.

4. Protección de Datos de los Usuarios:

- Cumplir con regulaciones de privacidad y protección de datos aplicables.

- Realizar auditorías de seguridad y pruebas de penetración regulares para identificar y remediar vulnerabilidades.

5. Control de Acceso al Sistema:

- Establecer políticas de acceso para garantizar que solo el personal autorizado tenga acceso al sistema de gestión de entrada.

- Registrar y auditar todas las acciones realizadas en el sistema.

6. Formación y Concienciación del Personal:

- Capacitar al personal en las prácticas seguras de gestión de entrada y en la identificación de posibles amenazas.

7. Respuesta ante Incidentes:

- Desarrollar un plan de respuesta a incidentes para abordar posibles violaciones de seguridad o interrupciones del sistema.

8. Actualizaciones y Mantenimiento:

- Mantener el sistema y el software actualizados para protegerlo contra vulnerabilidades conocidas.

9. Evaluación de Proveedores:

- Evaluar la seguridad de los proveedores de tecnología y servicios relacionados con el sistema de gestión de entrada.

* Políticas de Contraseña:
* Las contraseñas deben ser lo más complejas posible, utilizando una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.
* Se deben evitar contraseñas obvias como "password" o "123456".
* Se deben utilizar contraseñas de al menos 8 caracteres de longitud.
* Las contraseñas se guardan cifradas.
* Los usuarios nunca deben compartir sus contraseñas con otras personas, incluso dentro de la organización.
* No se deben escribir contraseñas en lugares visibles o fáciles de acceder.

### Detectar (DE):

Está vinculada a la definición y ejecución de las actividades apropiadas dirigidas a la identificación temprana de los incidentes de seguridad.

Las categorías dentro de esta función son: Anomalías y eventos; Monitoreo continuo de la seguridad; Procesos de detección.

### Responder (RE):

Está vinculada a la definición y ejecución de las actividades apropiadas para tomar medidas en caso de detección de un evento de seguridad. El objetivo es reducir el impacto de un potencial incidente de seguridad informática.

Las categorías dentro de esta función son: Planificación de la respuesta; Comunicaciones; Análisis; Mitigación; Mejoras.

### Recuperar (RE):

Está vinculada a la definición y ejecución de las actividades dirigidas a la gestión de los planes y actividades para restaurar los procesos y servicios deficientes debido a un incidente de seguridad. El objetivo es asegurar la resistencia de los sistemas e instalaciones y, en caso de incidentes, apoyar la recuperación oportuna de las operaciones.

Las categorías dentro de esta función son: Planificación de la recuperación; Mejoras y Comunicaciones.

### 