PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION EN EL IMRD CHIA

Después de realizar un análisis a la infraestructura de la entidad, a su personal, a sus activos
En ese orden de ideas se realizará un listado:

- Fundamentos de seguridad:
  Primero debemos saber a qué tipo de ataques estamos expuestos:

Término	Definición
Ataque dirigido	Un tipo de amenaza en la que los actores de amenazas persiguen y comprometen activamente la infraestructura de una entidad objetivo mientras mantienen el anonimato.
Ataque oportunista	Un ataque donde el actor de amenaza casi siempre está tratando de ganar dinero lo más rápido posible y con el mínimo esfuerzo.
Persona enterada	Un agente de amenazas que ha autorizado el acceso a una organización y que intencional o involuntariamente lleva a cabo un ataque.
Competidor	Un agente de amenazas que realiza ataques en nombre de una organización y se dirige a empresas competidoras.
Hacker	Cualquier agente de amenazas que utilice su conocimiento técnico para eludir la seguridad, explotar una vulnerabilidad y obtener acceso a información protegida.
Cibercriminal	Una subcategoría de agentes de amenazas de piratas informáticos que están dispuestos a tomar más riesgos y usar tácticas más extremas para obtener ganancias financieras.
Estado nacional	Un agente de amenaza que es un estado soberano que puede librar una guerra total contra un objetivo y tener recursos y dinero significativos a su disposición.
Amenaza interna	Una amenaza de personas autorizadas (personas con información privilegiada) que explotan sus privilegios inherentes para llevar a cabo un ataque.

Amenaza externa	Una amenaza de individuos o grupos que atacan una red desde el exterior y buscan obtener acceso no autorizado a los datos.
Amenaza Persistente	Una amenaza que busca acceder a una red y permanecer allí sin ser detectada.
Amenaza no persistente	Una amenaza en la que la única preocupación es ingresar a un sistema y robar información, y suele ser un evento único en el que el atacante no está preocupado si se nota su presencia.
Inteligencia de código abierto (OSINT)	Información que está disponible para el público y que no requiere ningún tipo de actividad maliciosa para obtenerla.

Luego de saber a qué tipos de ataques estamos expuestos realizamos un análisis de políticas y veremos si contamos con ellas o no.

- Políticas, procedimientos

Término	Definición	CUMPLIMOS	COMO
Regulación	Un requisito publicado por un gobierno u otro organismo de licencias que debe cumplirse.	SI	Todas las. Mintic
Procedimiento	Un proceso pasó a paso que describe cómo implementar una acción específica.	NO	
Base	Un estándar que dicta la configuración y los mecanismos de seguridad que se deben imponer en un sistema para cumplir con los estándares de seguridad requeridos.	SI	contamos con todos los manuales y lineamientos del ministerio de las TICs
Guía	Una recomendación que se utiliza cuando no existe una norma o procedimiento específico.	NO	

Política de uso aceptable (AUP)	Una política que define cómo los usuarios deben usar la información y los recursos de red en una organización.	NO	URGENTE
Política de privacidad	Una política que describe cómo la organización protegerá la información privada de los empleados, clientes y clientes.	NO	
Política de acceso autorizado (AAP)	Una política que especifica los controles de acceso que se emplean en una red.	NO	Cada nuevo acceso es autorizado por el jefe del área administrativa y financiera y/o director de la compañía.
Política de gestión de cambios y configuración	Una política que regula los cambios en las políticas, prácticas y equipos que podrían afectar la seguridad de su infraestructura de TI.	NO	formato para realizar los controles de cambio, es urgente implementarlo para cada área.
Política de seguridad organizacional	Una visión general de alto nivel del programa de seguridad corporativa.	NO	Debemos entender y ser conscientes de la seguridad corporativa no es un juego es muy importante
Política de contraseñas	Una política que detalla los requisitos para las contraseñas utilizadas en una organización.	NO	
Política de educación y conciencia del usuario	Una política con disposiciones para la formación del usuario y la formación en sensibilización.	NO	La formación dada por la policía nacional a funcionarios de la compañía.
Política de gestión de usuarios	Una política que identifica las acciones a seguir cuando el estado del empleado cambia para garantizar la seguridad del sistema, incluida la		Ojo, es muy importante.

	contratación de nuevos empleados, la promoción y transferencia de empleados y la terminación de empleados.	NO	

- Red

Término	Definición	CUMPLIMOS	COMO
Plan de red manejable	Un proceso creado para ayudar a hacer que una red sea manejable, defendible y segura.	SI	A través de políticas de seguridad de acceso
Hito	Una acción o evento que marca un cambio significativo al implementar un plan de red manejable.	SI	Con el mismo control de cambios.

INGENIERIA SOCIAL: podemos identificar e ignora los engaños del correo electrónico para proteger los recursos del sistema, capacitar al funcionario para que identifique los phishing. Para esto es muy importante tener claro los términos y definición:

Término	Definición
Ingeniería social	Un intento malicioso de adquirir de manera fraudulenta información confidencial que generalmente se realiza mediante la suplantación de personas.
Ingeniería social pasiva	Recopilar información o obtener acceso a áreas seguras aprovechando las acciones no intencionales de las personas.
Ingeniería social activa	Recopilación de información o acceso a áreas seguras a través de la interacción directa con los usuarios.
Surf de hombro	Mirar por encima del hombro de alguien que trabaja en una computadora para ver nombres de usuario, contraseñas o números de cuenta.

Escuchas	Escuchar una conversación entre empleados discutiendo temas delicados.
Buceo contenedor	El proceso de buscar en la basura información sensible que no se eliminó adecuadamente.
Navegación a cuestas	Entrar en un edificio seguro siguiendo a un empleado autorizado a través de una puerta segura sin proporcionar identificación.
Autoridad	Una técnica de ingeniería social activa que implica la personificación de autoridades legales, organizativas y sociales.
Intimidación	Una técnica de ingeniería social activa que usualmente involucra a un atacante que se hace pasar por un gerente o director para asustar a los empleados de niveles inferiores para obtener información.
Consenso	Una técnica de ingeniería social activa que aprovecha la disposición de las personas para realizar un acto si otros ya lo han hecho.
Escasez	Una técnica de ingeniería social activa que intenta hacer creer a las personas que, si no actúan con rapidez, perderán un elemento, una oportunidad o una experiencia.
Familiaridad	Una técnica de ingeniería social activa que aprovecha la disposición de las personas para realizar un acto solicitado por alguien con quien están familiarizados.
Urgencia	Una técnica de ingeniería social activa que intenta hacer que las personas crean que deben actuar con rapidez para evitar daños o sufrimientos inminentes.
Suplantación de identidad	Un ataque de ingeniería social que generalmente involucra el envío de correos electrónicos que se dice que son de compañías acreditadas para inducir a las personas a revelar información personal, como contraseñas y números de tarjetas de crédito.
Lanzar Phishing	Un ataque de ingeniería social dirigido a individuos específicos dentro de una empresa para obtener acceso a información que le permitirá al atacante obtener una ventaja comercial o cometer un fraude.
Ballenero	Un ataque de phishing dirigido a objetivos de altos ejecutivos y víctimas de alto perfil.

Vishing	Un ataque de ingeniería social que explota los servicios de telefonía de voz sobre IP para obtener acceso a la información personal y financiera de una persona, incluido su número de identificación gubernamental, números de cuentas bancarias o números de tarjetas de crédito.
Correo electrónico Hoax	Un ataque de ingeniería social que ataca a los destinatarios de correos electrónicos que tienen miedo y creerán en la mayoría de la información si se presenta de manera profesional.
Virus Hoax	Informes falsos sobre virus inexistentes que a menudo dicen hacer cosas imposibles que hacen que los destinatarios tomen medidas drásticas, como apagar su red.
Abrevadero	Un ataque de ingeniería social donde la víctima es un grupo como una organización, una industria o una región y donde la atacante adivina u observa qué sitios web usa e infecta uno o más de ellos con malware.

Estas definiciones de ataques son divulgadas por un ingeniero intendente de la policía nacional de Colombia con experiencia en ataques informáticos. (se solicita acercamiento con este para poder dar una charla a todos los empleados con acercamiento a equipos tecnológicos).

Seguridad Física:

Término	Definición	CUMPLIMOS	COMO
Seguridad física	La protección de los activos corporativos contra amenazas tales como robo o daño.	SI	contamos con seguridad privada.
Prevención	Haciendo un lugar menos tentador para entrar.	SI	Se cuenta con acceso restringido mediante seguridad privada.
Detección	La identificación de la intrusión, los activos faltantes alcance de cualquier daño.	NO	Contamos con equipos como, impresoras expuestas a tuberías, goteras y manipulación de personal no autorizado
Recuperación	La revisión de los procedimientos de seguridad		No se realizan arreglos definitivos sino parciales.

	física, la reparación de cualquier daño y el fortalecimiento de la seguridad física contra problemas futuros.	NO	No se tiene en cuenta la seguridad física.
Barreras perimetrales	Dispositivos y procedimientos de seguridad física que protegen el límite exterior de una instalación.	SI	Se cuenta con personal de vigilancia el 7 * 24 * 365 días del año.
Circuito cerrado de televisión (CCTV)	Un sistema de televisión en el que las señales no se distribuyen públicamente, sino que se monitorean, principalmente con fines de vigilancia y seguridad.	NO	No se cuenta con este servicio ni dispositivos.
Controles de acceso físico	Cercas, torniquetes, teclados y otros dispositivos que controlan el acceso a una instalación.	SI	Se cuenta con biometría para control de para control de acceso. Y vigilancia privada, las puertas de acceso a la compañía permanecen abiertas.

AMENAZA DE RED:

Término	**Definición**
Ataque activo	Un ataque donde los perpetradores intentan comprometer o afectar las operaciones de un sistema de alguna manera.
Ataque pasivo	Un ataque donde los perpetradores intentan recopilar información sin afectar el flujo de esa información desde la red objetivo.
Ataque externo	Un ataque donde personas no autorizadas intentan romper una red desde fuera del sitio.
Ataque interno	Un ataque iniciado por personas autorizadas dentro del perímetro de seguridad de la red que intentan acceder a sistemas o recursos para los cuales no están autorizados.

Punto de entrada	Una ubicación o dispositivo que es vulnerable a los ataques.
Línea de base de red	La actividad normal de la red, incluidos los patrones de tráfico típicos, el uso de datos y las cargas del servidor, se utiliza para identificar una actividad inusual o atípica, lo que puede indicar un ataque.
Segmentación de la red	Dividir una red en segmentos por razones de rendimiento o seguridad.

SEGURIDAD DE LA RED:

Término	Definición	CUMPLIMOS	COMO
LAN virtual (VLAN)	Un agrupamiento lógico de computadoras basado en el puerto del switch.	SI	Contamos con DMZ implementado en la red
Tabla de memoria direccionarle de contenido (CAM)	Una tabla mantenida por un conmutador que contiene direcciones MAC y sus ubicaciones de puerto correspondientes.	SI	Se cuenta con utm que realiza las veces de conmutador, se está organizando ip mapeada a x Mac address.

Host: normalmente se reciben ataques a los host o computadores, sean de escritorio, todo en uno portátiles etc. A continuación, aparecerán un listado de los ataques más comunes y si cumplimos con el software o el antivirus necesarios para impedir o mitigar estos ataques. También contamos con una excelente configuración de Windows defenders

Término	Definición	CUMPLIMOS	COMO
Malware	Software diseñado para hacerse cargo o dañar una computadora sin el conocimiento o aprobación del usuario.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos

			USB para evitar contaminación desde fuera de la empresa. excelente configuración de Windows defender
Virus	Un programa que intenta dañar un sistema informático y replicarse a otros sistemas informáticos.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa. excelente configuración de Windows defender
Gusano	Un programa de autoreplicación.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa excelente configuración de Windows defender
Caballo de Troya	Un programa malicioso disfrazado de software legítimo o deseable.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa

			excelente configuración de Windows defender
Zombi	Una computadora que está infectada con malware que permite actualizaciones de software remotas y control por un centro de comando y control llamado un maestro zombie.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa excelente configuración de Windows defender
Botnet	Un grupo de computadoras zombie que son comandadas desde una infraestructura de control central.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa excelente configuración de Windows defender
Rootkit	Un conjunto de programas que permite a los atacantes mantener un acceso permanente, a nivel de administrador, oculto a una computadora.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa excelente configuración de Windows defender

Bomba lógica	Malware diseñado para ejecutarse solo en condiciones predefinidas que permanecen inactivas hasta que se cumple la condición predefinida.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa excelente configuración de Windows defender
Spyware	El software que se instala sin el consentimiento o conocimiento del usuario y está diseñado para interceptar o tomar control parcial sobre la interacción del usuario con la computadora.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa excelente configuración de Windows defender
Adware	Malware que supervisa acciones que denotan preferencias personales y envía ventanas emergentes y anuncios que coinciden con esas preferencias.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa excelente configuración de Windows defender
Ransomware	Malware que niega el acceso a un sistema informático hasta que el usuario paga un rescate.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral

			desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa excelente configuración de Windows defender
Scareware	Una estafa para engañar a los usuarios y hacerles creer que tienen algún tipo de malware en su sistema.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa excelente configuración de Windows defender
Crimeware	Malware diseñado para perpetrar el robo de identidad para permitir el acceso a cuentas en línea en servicios financieros, como bancos y minoristas en línea.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa excelente configuración de Windows defender
Crypto-Malware	Ransomware que encripta archivos hasta que se paga un rescate.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall utm fortigate 100E, además se bloquean los puertos USB para evitar

			contaminación desde fuera de la empresa excelente configuración de Windows defender
Troyano de acceso remoto(RAT)	Malware que incluye una puerta trasera que permite el control administrativo sobre la computadora de destino.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa excelente configuración de Windows defender
Hacker	Una persona que comete delitos informáticos y cibernéticos al obtener acceso no autorizado a los sistemas informáticos.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa excelente configuración de Windows defender
Galleta	Una persona que participa activamente en el desarrollo y la distribución de gusanos, troyanos y virus, participa en actividades de sondeo y reconocimiento, crea conjuntos de herramientas para que otros puedan hackear vulnerabilidades conocidas y rompa medidas de protección.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa

			excelente configuración de Windows defender
Script Kiddy	Un hacker menos capacitado (generalmente más joven) que a menudo se basa en herramientas o scripts automatizados escritos por crackers para escanear sistemas al azar para encontrar y explotar las debilidades.	SI	Contamos con consola de antivirus BITDEFENDER y antivirus perimetral desde le firewall fortigate 100E, además se bloquean los puertos USB para evitar contaminación desde fuera de la empresa excelente configuración de Windows defender

GESTION DE DATOS:

Termino	Definición	CUMPLIMOS	COMO
Clasificación de la información	El proceso de determinar qué información se divulgará y cómo divulgarla para garantizar los requisitos de privacidad de una organización.	Si	Solo se divulga información que sea de interés público por ley de transparencia.
Custodio de datos	Una persona que es responsable de la calidad de los datos en el día a día.	Si	Cada funcionario en el cumplimiento de sus funciones debe velar por la calidad de los datos actualizados y almacenados.

Productor de datos	Una persona responsable de crear o capturar datos. La mayoría de las personas en una organización son productores de datos.	Si	En la entidad se cuenta con aproximadamente 34 funcionarios que tienen relación directa con la captura y creación de datos.
Consumidor de datos	Una persona que usa datos.	Si	Aquellos funcionarios que toman información de los sistemas de información implementados y los usuarios externos que consultan la página Web.
Oficial de Privacidad	Una persona que supervisa las actividades de datos para garantizar que cumplen con las leyes gubernamentales.	No	
Pulpeando	Un método para eliminar todos los rastros de tinta del papel utilizando productos químicos y luego triturando el papel en la pulpa.	NO	
Pulverizando	Utilizando un sistema de punzonadora o martillo para destruir un dispositivo de	No	

	almacenamiento de datos.		
Degaussing	Purga un disco duro exponiéndolo a pulsos magnéticos altos que destruyen todos los datos en el disco.	No	
Purga	La eliminación de datos confidenciales, asegurándose de que los datos no puedan reconstruirse con ninguna técnica conocida.	No	
Limpiando	Un método basado en software de sobrescribir datos para destruir completamente todos los datos electrónicos que residen en una unidad de disco duro u otro medio digital.	No	

IMPLEMENTACIONES CRIPTOGRAFICAS

Término	Definición	CUMPLIMOS	COMO
Criptografía simétrica	Un método de cifrado que utiliza una sola clave tanto para	NO	

	el cifrado como para el descifrado.		
Criptografía asimétrica	Un método de cifrado que utiliza dos claves diferentes pero relacionadas matemáticamente, una para el cifrado y otra para el descifrado.	SI	Se pueden utilizar los tokens para los bancos
Firma digital	Una combinación de cifrado asimétrico y valores de hashing que proporcionan confidencialidad, validación de integridad, autenticación sólida y no repudio.	NO	
Sobre digital	Un método para utilizar el cifrado asimétrico para proteger un mensaje antes de enviarlo al destinatario.	NO	Aunque ya google cuenta con este servicio, se debe contratar.
Módulo de plataforma confiable (TMP)	Un chip de hardware en la placa base que puede generar y almacenar claves criptográficas.	NO	
Módulo de seguridad de hardware (HSM)	Una pieza de hardware y software / firmware asociado que está conectado a un sistema informático para proporcionar funciones criptográficas como cifrado, descifrado, generación de claves y hashing.	NO	

ALMACENAMIENTO EN LA NUBE

Término	Definición	CUMPLIMOS	COMO
Almacenamiento en la nube	Un modelo de almacenamiento de datos que un tercero generalmente proporciona como un servicio.	SI	correos Google.
Corredor de seguridad de acceso a la nube (CASB)	Una herramienta o servicio de software que actúa como un controlador de acceso, lo que permite a la organización extender el alcance de sus políticas de seguridad a la infraestructura de almacenamiento en la nube.	SI	Google drive con todas sus políticas de seguridad.

Atentamente,

ALDOVER ALEXANDER COLORADO
Director General IMRD Chía

Elaboro: Fabian Romero - Prof. Universitario
Reviso: Narda López-subdirectora Adm y Financiera