SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

1.8.1 SEGURIDAD DE TI / GOBERNANZA DE LA CIBERSEGURIDAD

Para Protección S.A. la seguridad de los sistemas de información corporativos y de clientes es de gran importancia y hace parte de las estrategias claves para construir la confianza en los servicios, y lograr la sostenibilidad organizacional y del sistema del cual hacemos parte en la administración y gestión de los fondos y las inversiones para el bienestar futuro y presente de nuestros clientes.

Todas las instancias de la organización están comprometidas con el aseguramiento de los sistemas y la información. La alta dirección y la junta directiva han definido todas las políticas y destinado los recursos necesarios para que se implementen los mecanismos de seguridad de los sistemas de información. La ciberseguridad es parte de la agenda de trabajo de los comités ejecutivos y estratégicos.

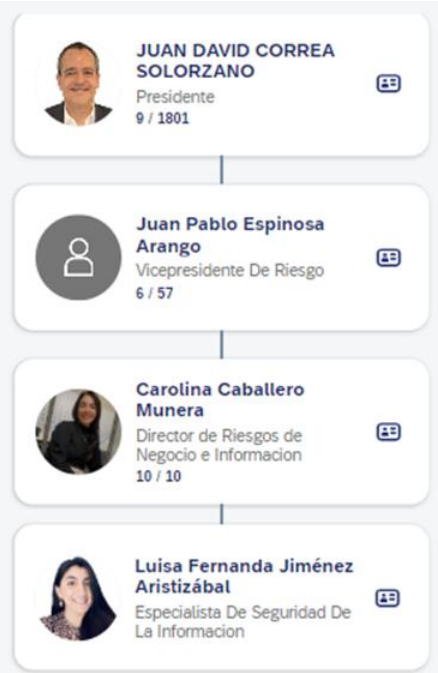
Para prevenir los impactos, responder con diligencia y generar un impacto positivo en los grupos de interés, la compañía ha implementado una estructura con responsabilidades claras en cuanto a la gestión de riesgos, seguridad de la información, ciberseguridad, todo dentro de un marco de control interno articulado de manera consistente. Se han implementado controles para el ciclo de vida de las soluciones de TI, la seguridad en los accesos, gestión del monitoreo y gestión de la ciberseguridad, así como planes de resiliencia con respaldos y un DRP (Disaster Recovery Plan) que es probado anualmente. Por ser una empresa bajo la supervisión de las autoridades financieras, cuenta con procesos maduros para la gestión de buenas prácticas, regulación y normativa. Para garantizar que nuestros proveedores cuentan con los mismos niveles de seguridad, se hace un monitoreo permanente a los aliados estratégicos.

En los últimos 3 años, la organización ha invertido un rubro importante en la implementación de tecnologías de protección para gestión de la ciberseguridad y la seguridad de la información con el apoyo de empresas de talla mundial como Microsoft y Palo Alto, entre otras. Y en el último año, tanto la Inteligencia Artificial como la gestión basada en riesgos, han sido parte de las iniciativas del mejoramiento continuo.

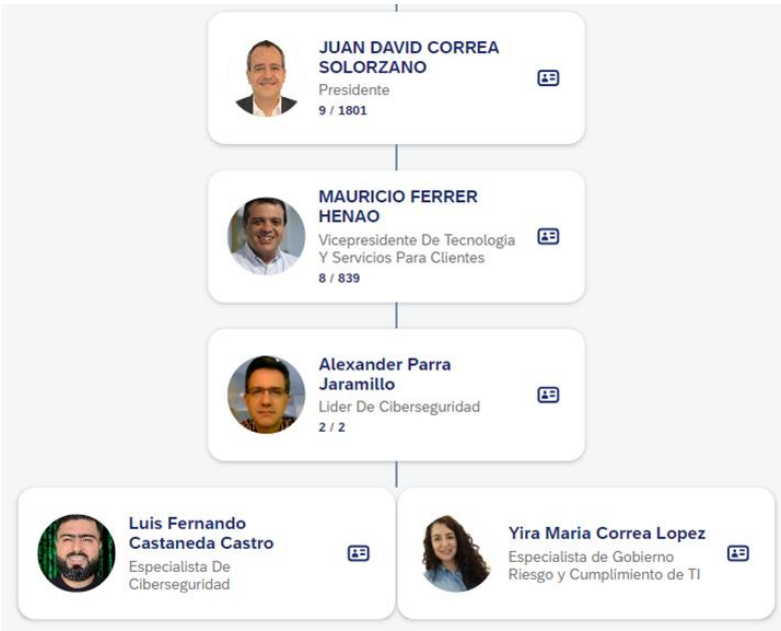
Organigrama Seguridad de la Información

La organización cuenta con una estructura de personal calificado para la gestión de la seguridad de la información y la ciberseguridad:

Organigrama Seguridad de la Información:



Organigrama Seguridad de TI (Ciberseguridad):



*En el equipo de Seguridad de TI existe una vacante adicional que está en proceso de selección: Especialista de Seguridad Gestionada

Otras instancias en la estructura que participan activamente en el gobierno para la seguridad de la información y ciberseguridad:

- **JUNTA DIRECTIVA – COMITÉ DE RIESGO**
  - En la agenda anual del comité de riesgos de Junta se hace revisión de los planes y avances en materia de seguridad de información y ciberseguridad.
- **PRESIDENCIA – Comité directivo**
  - En la agenda anual del comité de presidencia se incluye la materia de seguridad de información y ciberseguridad.
- **COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD**
  - Protección S.A. cuenta con un Comité de Seguridad de la Información y Ciberseguridad, el cual es responsable de asegurar que exista una dirección y apoyo gerencial para soportar la formulación, desarrollo y mantenimiento del Modelo de Seguridad de la Información y Ciberseguridad y sus iniciativas relacionadas
- **OFICIAL DE SEGURIDAD DE LA INFORMACIÓN**
  - Protección S.A. cuenta con un CISO, responsable de crear, implementar y supervisar el Modelo de Seguridad de la Información, y alinearse con el Programa de Ciberseguridad. El ciso está al frente del área de seguridad de información bajo la sombrilla de la gestión de riesgos de negocio.
- **VICEPRESIDENCIA DE TECNOLOGIA Y SERVICIOS PARA LOS CLIENTES**
  - En la VP de tecnología y servicios para clientes se cuenta con el área de seguridad de TI que se ocupa de los siguientes aspectos:
    - Gobierno, riesgo y cumplimiento de TI
    - Seguridad en el ciclo de vida de las soluciones y los canales de TI
    - Seguridad para la gestión de accesos
    - Gestión de las herramientas de seguridad y primer nivel de monitoreo y respuesta
    - Ciberseguridad, monitoreo y respuesta a incidentes
- **UNIDAD DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD**
  - El área de Seguridad de Tecnologías de Información (TI), gestiona los riesgos de seguridad de ciberseguridad e implementa los controles adecuados para los activos de información en los sistemas de la organización. El área de Seguridad de la Información es responsable de definir las Políticas asociadas a seguridad de la información y de manera correspondiente el proceso de seguridad de TI define las políticas específicas asociadas.

1.8.2 METRICAS DE LA SEGURIDAD DE TI Y CIBERSEGURIDAD

En Protección S.A. trabajamos para proteger la información y todos los activos que soportan su gestión, mediante la preservación de los principios de Confidencialidad, Integridad y Disponibilidad, contando con el compromiso de todos los colaboradores, proveedores y terceros relacionados.

Esta Política establece los lineamientos generales en materia de seguridad de la información y ciberseguridad, por lo anterior, se define como objetivo establecer un

modelo de gobierno para la protección de la información y sus activos asociados, contra las diversas fuentes de riesgo derivados del manejo de estos activos.

Todos los empleados realizan un curso anual de riesgos, gobierno y seguridad de la información y TI, el cual es evaluado y contribuye a uno de los indicadores de desempeño. En los contratos se establecen las responsabilidades y sanciones en materia de seguridad de la información y se realizan las respectivas investigaciones y procesos disciplinarios de manera formal.

- **Una política de seguridad de la información / ciberseguridad está disponible internamente para todos los empleados:** La organización a establecido procesos para una adecuada gestión de la seguridad en los sistemas de información que se utilizan en todas las áreas de la compañía. Esto exige un alto compromiso en las inversiones y la disposición de equipos de trabajo calificados que evalúan las necesidades en los diferentes procesos de la organización, incorporan los mecanismos y controles de seguridad necesarios en todo el ciclo de vida de los elementos tecnológicos de información y realizan un monitoreo constante para identificar nuevos riesgos y gestionarlos adecuadamente
- **Capacitación en concientización sobre seguridad de la información:** Todos los empleados realizan un curso anual de riesgos, gobierno y seguridad de la información y TI, el cual es evaluado y contribuye a uno de los indicadores de desempeño.
- **Un proceso de escalamiento claro que los empleados pueden seguir en caso de que un empleado note que algo sospechoso está en su lugar:** El Equipo de Ciberseguridad monitorea de manera continua y proactiva, para la detección de eventos de seguridad de la información que podrían representar un riesgo para Protección S.A. Así mismo, todo el personal interno y externo de Protección S.A debe estar en capacidad de identificar y notificar las señales de un potencial incidente. El inicio del incidente de seguridad de la información se da cuando se detecta o se reporta a través de: • Alertas automáticas y sistemas de monitoreo • Reportes mediante 1. llamadas telefónicas 2. informes al Centro de Servicios Corporativo. 3. Correos electrónicos a segurinfo@proteccion.com.co Seguridad.informacion@proteccion.com.co. El responsable de gestionar el incidente registra el incidente en la herramienta disponible para la gestión y seguimiento de incidentes de seguridad
- **La seguridad de la información / ciberseguridad es parte de la evaluación del desempeño de los empleados (por ejemplo, acciones disciplinarias):** Si bien no se cuenta con una evaluación directa del desempeño asociado a la seguridad de la información si se cuenta con una medida donde todos los empleados realizan un curso anual de riesgos, gobierno y seguridad de la información y TI, el cual es evaluado y contribuye a uno de los indicadores de desempeño. En los contratos se establecen las responsabilidades y sanciones en materia de seguridad de la información.

ANEXO: Política de seguridad de la información y ciberseguridad

PROCESO E INFRAESTRUCTURA

1. **PLANES DE CONTINUIDAD DEL NEGOCIO:**
   La Organización cuenta con una estructura, procesos y herramientas para la gestión del plan de continuidad de los negocios. Bajo la dirección del área de Riesgos de Negocio y Seguridad de información, existe un rol dedicado a la gestión y revisión anual de la estrategia del plan de continuidad de negocio que articula a los demás equipos y áreas de apoyo tales como: Seguridad de las personas y comité de emergencias, operación de Ti y Disaster Recovery Plan (DRP), gestión administrativa para la coordinación de los recursos mínimos de recuperación, y los equipos de procesos de negocio para establecimiento de la estrategia de análisis de negocio y BIA. Los planes de continuidad y las estrategias de los diferentes grupos que lo articulan son probados al menos una vez al año.

   Durante el mes de mayo se realizo una prueba de continuidad del negocio donde el escenario de prueba buscaba 1. Validar para el core de voluntarias AFP Core y la interacción con los demás servicios de tecnología como este 2. Carga operativa real y con días hábiles

   Las conclusiones de esta prueba fueron:
   - Actividad exitosa, se soporta la operación con carga normal, en días hábiles con todos los canales habilitados
   - Todos los incidentes presentados se resolvieron durante los días de la prueba
   - Se listan actividades que serán adelantadas durante 2024 para validar causales y dar soluciones de raíz o para mejorar los procesos
   - Existen actividades que deben ser automatizadas en pro de evitar errores humanos o disminuir el RTO. RTO actual de 3.55 horas

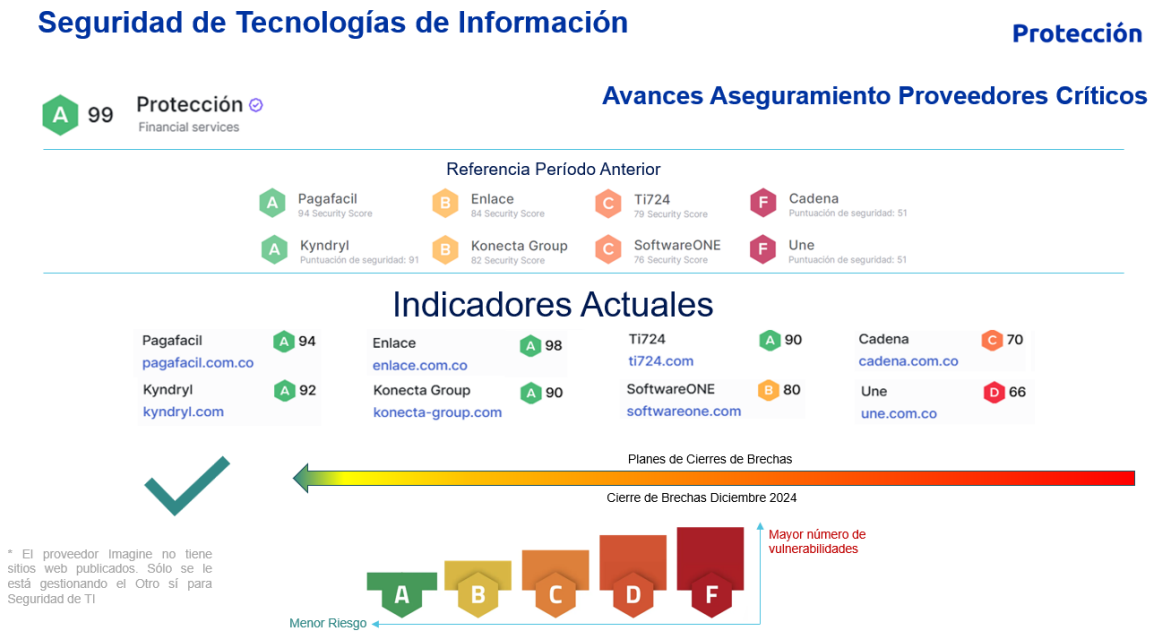
2. **CERTIFICACIONES:**
   La organización tiene como referencia los estándares de la ISO27000, NIST, COBIT, para la gestión de los riesgos y controles de la seguridad en los activos de información y tecnología. Los procesos de vigilancia de las entidades de control nacional como la superintendencia financiera, los marcos de cumplimiento como SOX, y la obligatoriedad de protección de los datos personales, le han dado a la organización un alto nivel de madurez en la adopción de los marcos estándares para la gestión de los controles generales de TI y de la información.

3. **VERIFICACIÓN EXTERNA Y ANALISIS DE VULNERABILIDADES:**
   La organización cuenta con servicios contratados de empresas especializadas en la evaluación y análisis de vulnerabilidades. La firma encargada de ésta

responsabilidad es Deloitte, respaldada por su trayectoria en materia de auditoría de sistemas de información y controles generales de tecnología.

- Auditoria externa: a la espera de carta deloitte

La siguiente es la imagen que muestra el estado de aseguramiento de Protección y sus aliados, evidencia de la gestión en materia de gestión adecuada de vulnerabilidades, hacking y seguridad de terceros



4. VIOLACIONES

La organización cuenta con servicios especializados para el monitoreo y respuesta a la gestión de eventos de seguridad de las plataformas y servicios de tecnologías de información. Durante el período se identifican y contienen los eventos, mitigando la probabilidad e impacto de un incidente real de seguridad.

	2021	2022	2023	2024
Numero total de violaciones de seguridad de la información	0	0	0	0
Numero total de clientes, consumidores y empleados impactados por las violaciones	0	0	0	0