PROGRAMA Y PLAN ESTRATEGICO DE CIBERSEGURIDAD

Grupo Empresarial Argos

Programa, Estrategia y Modelo de Gestión Integral de Ciberseguridad

1. Introducción

En un mundo interconectado y digitalizado, la ciberseguridad se ha convertido en un pilar fundamental para el éxito y la sostenibilidad de cualquier organización. En el caso del Grupo Empresarial Argos, que opera en más de 18 países y abarca 10 industrias diferentes, la protección de los activos de información frente a los riesgos cibernéticos se vuelve aún más crucial. Este programa, estrategia y modelo de gestión integral de ciberseguridad tienen como objetivo proporcionar una visión estratégica y una articulación organizada de los elementos y medidas necesarias para proteger nuestros activos de información en un entorno global altamente digitalizado y disperso.

2. Visión Estratégica

La visión estratégica de nuestra estrategia de ciberseguridad es ser líderes en la protección de los activos de información del Grupo Empresarial Argos, manteniendo la confianza y seguridad digital de nuestros clientes y usuarios. Esto se logrará a través de la identificación y articulación organizada de los riesgos cibernéticos, la implementación de medidas preventivas y correctivas efectivas, y el fortalecimiento continuo de nuestras capacidades en ciberseguridad.

3. Desafíos y Cuestionamientos

El desarrollo del programa y estrategia de ciberseguridad busca abordar los siguientes desafíos y cuestionamientos clave, considerando la complejidad y dispersión operativa del Grupo Empresarial:

Identificación y Control de Activos Críticos: ¿Cómo identificar, catalogar y proteger los activos de información críticos en un entorno global altamente digitalizado y disperso, incorporando la gestión de identidades no humanas y la preparación para amenazas cuánticas?

Identificación de Riesgos y Tratamiento: ¿Cómo identificar y priorizar los riesgos de ciberseguridad, incluyendo aquellos potenciados por IA y amenazas cuánticas, y asignar esquemas de tratamiento que aborden la dispersión operativa, la interdependencia con proveedores y la necesidad de gobernabilidad ética de la IA?

Prevención y Detección de Amenazas: ¿Qué herramientas y estrategias implementar para prevenir y detectar amenazas avanzadas potenciadas por IA, como deepfakes y ataques sin malware, mientras se abordan los riesgos sistémicos derivados de la dispersión tecnológica y las interdependencias del grupo empresarial?

Continuidad de Operaciones: ¿Cómo definir e implementar un plan de continuidad de operaciones frente a la materialización de un ataque cibernético, considerando las diferentes industrias y la falta de unidad en la respuesta a los riesgos? ¿Cómo diseñar e implementar un plan de continuidad de operaciones que integre resiliencia frente a ataques cibernéticos avanzados, como ransomware dirigido a sistemas industriales y amenazas cuánticas, asegurando una respuesta unificada en un grupo empresarial diverso?

Cultura de Ciberseguridad y Concienciación Ética: ¿Cómo fomentar una cultura de ciberseguridad que promueva la concienciación ética y la responsabilidad compartida en todas las compañías del grupo, considerando las diferencias culturales y operativas?

Articulación Organizacional: ¿Cómo articular todas las áreas de las diferentes compañías del grupo empresarial en función de la ciberseguridad, considerando la definición de roles y responsabilidades, fomentando una cultura de colaboración, integrando la gobernabilidad ética de la IA y preparando a la organización para amenazas cuánticas y avanzadas bajo un único esquema de trabajo corporativo?

4. Ventajas Competitivas de la Ciberseguridad

La implementación de una estrategia de ciberseguridad sólida ofrece diversas ventajas competitivas para el Grupo Empresarial, incluyendo:

Incursión en Nuevos Mercados: Facilita la entrada en mercados internacionales que requieran el cumplimiento de normas de ciberseguridad. Cumplir normas globales de ciberseguridad (como GDPR) facilita entrar a mercados internacionales. Ofrecer servicios como *Zero Trust* y soluciones contra amenazas cuánticas (siguiendo NIST) atrae clientes en sectores regulados como salud o finanzas.

Mayor Productividad: Limita las posibilidades de ataques exitosos, reduciendo el tiempo de recuperación y minimizando pérdidas económicas y de reputación.

Ventaja Competitiva: Garantiza el buen manejo de información sensible, manteniendo la preferencia y confianza de los usuarios.

Mejora del Servicio al Cliente: Incrementa la eficiencia y automatización de soluciones, mejorando la satisfacción de los clientes.

Eficiencia en el Uso de Recursos: Permite el uso apropiado de los recursos, evitando costos adicionales y mejorando la eficiencia operativa.

Liderazgo en innovación: Posiciona al grupo empresarial como pionero en la adopción de tecnologías emergentes, como IA ética y criptografía poscuántica, permitiendo ofrecer servicios innovadores a clientes externos.

Cultura ética y colaborativa: Promueve una cultura de ciberseguridad con formación que fortalece la confianza interna y externa.

5. Alcance del Sistema de Gestión de Ciberseguridad

El alcance del sistema de Gestión de Ciberseguridad abarca los servicios prestados a las compañías del grupo empresarial, los procesos de la Cadena de Valor y habilitadores incluidos:

Manufactura de cementos y concretos:

- Seguridad de los sistemas de control industrial (ICS): Proteger los sistemas de control industrial utilizados en la fabricación de cemento y concreto contra intrusiones y ataques cibernéticos.
- Seguridad de la cadena de suministro: Garantizar la integridad y seguridad de los sistemas y datos en toda la cadena de suministro, desde la adquisición de materias primas hasta la distribución de productos.
- Seguridad de la propiedad intelectual: Proteger los diseños, procesos y tecnologías propietarias utilizadas en la fabricación de cemento y concreto contra el robo o la manipulación.
- Resiliencia operativa: Implementar medidas para garantizar la continuidad operativa en caso de ataques cibernéticos que podrían afectar la producción y la entrega de productos.

Generación, distribución y comercialización de Energía:

- Protección de infraestructuras críticas: Asegurar la protección de los activos de infraestructura crítica, como centrales eléctricas, subestaciones y redes de distribución, contra ataques cibernéticos que podrían interrumpir el suministro de energía.
- Resiliencia del sistema eléctrico: Implementar medidas para garantizar la resiliencia del sistema eléctrico ante posibles amenazas cibernéticas, incluida la capacidad de respuesta y recuperación rápida después de un incidente.
- Seguridad de los datos del cliente: Proteger la información confidencial de los clientes, como datos de facturación y consumo de energía, contra accesos no autorizados y robo de datos.
- Cumplimiento normativo: Cumplir con los requisitos regulatorios específicos del sector energético en lo que respecta a la seguridad cibernética y la protección de datos.

Administración de Concesiones viales (Peajes) y Aeroportuarios (Aeropuertos):

- Seguridad de los sistemas de pago: Proteger los sistemas de pago utilizados en los peajes y aeropuertos contra fraudes y ataques cibernéticos que podrían comprometer la información financiera de los usuarios.
- Seguridad de la infraestructura de transporte: Asegurar la integridad y disponibilidad de la infraestructura de transporte, incluidas las carreteras y las instalaciones aeroportuarias, contra posibles amenazas cibernéticas que podrían afectar la seguridad pública.
- Seguridad de las comunicaciones: Proteger las redes de comunicaciones utilizadas para la gestión y operación de los peajes y aeropuertos contra intrusiones y accesos no autorizados.

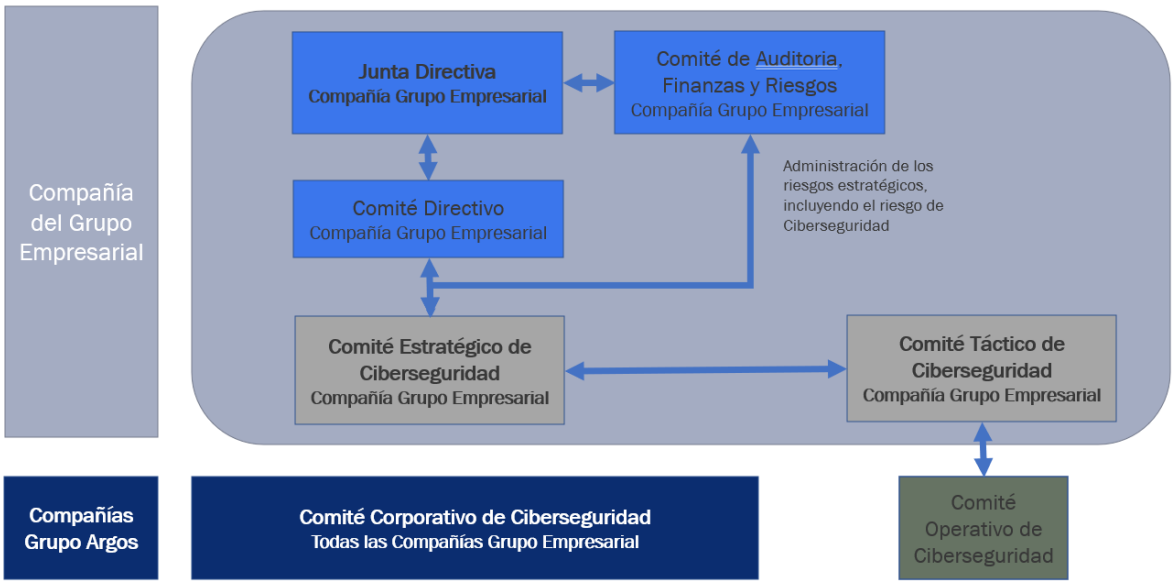
- Gestión de crisis: Establecer planes de respuesta a incidentes y protocolos de gestión de crisis para abordar rápidamente cualquier interrupción o incidente cibernético que pueda afectar las operaciones de transporte.

Inversiones financieras en Infraestructura:

- Seguridad de las transacciones financieras: Proteger las transacciones y los datos financieros confidenciales contra fraudes y ataques cibernéticos que podrían comprometer la integridad y la confidencialidad de la información.
- Gestión de riesgos financieros: Identificar y mitigar los riesgos cibernéticos que podrían afectar la estabilidad financiera y la reputación de las inversiones en infraestructura.
- Cumplimiento normativo: Cumplir con los requisitos regulatorios específicos del sector financiero en lo que respecta a la seguridad cibernética y la protección de datos financieros y personales de los clientes.
- Resiliencia del sistema financiero: Implementar medidas para garantizar la resiliencia del sistema financiero ante posibles amenazas cibernéticas, incluida la capacidad de recuperación después de un incidente.

6. Gobierno y Responsabilidades de Ciberseguridad

El gobierno de la ciberseguridad en el grupo empresarial se fundamenta en un claro respaldo y apoyo por parte de las directivas de las compañías. Este enfoque se materializa a través de diversas instancias y roles clave que colaboran en la gestión integral de la ciberseguridad.



Juntas Directivas:

Las juntas directivas asumen la responsabilidad primordial de la adopción y correcta implementación de políticas y normas de ciberseguridad. Además, establecen una estructura organizacional que brinda orientación y dirección para la gestión de la ciberseguridad. Asignan los recursos necesarios y ejercen un liderazgo efectivo para mitigar los riesgos digitales en la organización.

Comité Estratégico de Ciberseguridad:

Este comité desempeña un papel fundamental al aprobar la estrategia organizacional en la gestión de la ciberseguridad. También valida la política de ciberseguridad y sus lineamientos, gestiona el mapa de riesgos y evalúa la efectividad de las medidas de tratamiento adoptadas. Además, supervisa la adopción de recomendaciones emitidas por entidades de control y reporta regularmente a la junta directiva y a la alta dirección.

Comité Táctico de Ciberseguridad:

El Comité Táctico se encarga de materializar la política de ciberseguridad a través de la propuesta de lineamientos operativos. Monitorea constantemente el entorno cibernético para identificar riesgos y vulnerabilidades, supervisa la implementación de medidas de seguridad y diseña programas de pruebas de intrusión y simulacros ante ataques cibernéticos. Además, se encarga de ajustar los programas de capacitación y conciencia, así como de comunicar y reportar el estado de la ciberseguridad a la alta gerencia y otros miembros clave de la organización.

Propietarios y Custodios de Activos de Información y Ciberactivos:

Los propietarios son responsables de los activos asignados, incluyendo su clasificación, control y monitoreo. Mientras que los custodios garantizan la protección de los activos, haciendo cumplir las restricciones y clasificaciones de acceso establecidas por los propietarios.

Áreas de Control (Tecnología, Riesgos, Auditoría):

Estas áreas son responsables de gestionar y evaluar las medidas adoptadas para mitigar el riesgo asociado a la ciberseguridad, desde la perspectiva tecnológica, de riesgos y auditoría.

Oficial de Ciberseguridad (CISO):

Es el encargado de desarrollar un modelo integral de gestión de ciberseguridad, enmarcando la política de ciberseguridad dentro de este ecosistema. Su labor se centra en la gestión de riesgos asociados a la seguridad de la información y la ciberseguridad, además de diseñar y gestionar el programa de Ciberseguridad con el fin de asegurar el control interno basado en tecnologías de la información y articular las necesidades del negocio para una transformación digital segura, preservando la sostenibilidad de las organizaciones del grupo empresarial en el mercado. El rol establece las arquitecturas y controles en los procesos, tecnologías y personas que sean relevantes para la mitigación de riesgos y protección de los activos de información. Esta

labor se fundamenta en prácticas de seguridad, estándares y regulaciones internacionales que rigen a las empresas del grupo empresarial.

Usuarios:

Todos los colaboradores, proveedores, contratistas y terceros autorizados que utilizan la información de las compañías en el desempeño de sus actividades diarias son considerados usuarios y juegan un papel crucial en la protección de los activos de la organización.

7. Políticas y Lineamientos de Ciberseguridad

Las políticas y lineamientos de ciberseguridad del grupo empresarial representan el compromiso de la dirección con la protección de la información y los activos digitales, así como con la mitigación de los riesgos asociados a las amenazas cibernéticas. Estas directrices están respaldadas por estándares reconocidos internacionalmente y por las mejores prácticas de la industria, incluyendo la normativa ISO/IEC 27000 y los controles del Centro de Seguridad de la Información (CIS). Véase: Política de Ciberseguridad

Normativa ISO/IEC 27000:

La serie de normas ISO/IEC 27000 establece un marco integral para la gestión de la seguridad de la información, proporcionando estándares, directrices y mejores prácticas para la implementación de sistemas de gestión de la seguridad de la información (SGSI). La política de ciberseguridad del grupo empresarial se basa en los principios y requisitos de la norma ISO/IEC 27001, la cual establece criterios para establecer, implementar, mantener y mejorar continuamente un SGSI basado en un enfoque de gestión de riesgos.

Controles CIS (Centro de Seguridad de la Información):

Los Controles CIS son un conjunto de mejores prácticas de seguridad de la información desarrolladas por el Centro de Seguridad de la Información. Estos controles proporcionan un conjunto conciso de acciones específicas para mejorar la ciberseguridad de una organización. La política de ciberseguridad del grupo empresarial incorpora los controles CIS como parte integral de su enfoque de seguridad, utilizando estos lineamientos para definir medidas específicas y procesos de gestión alineados con las mejores prácticas reconocidas a nivel internacional.

Integración en Políticas, Lineamientos y Anexos:

Las políticas, lineamientos y anexos de ciberseguridad del grupo empresarial se basan en la normativa ISO/IEC 27000 y los controles CIS, asegurando que reflejen los estándares más rigurosos y actualizados en materia de ciberseguridad. Al integrar estas referencias, el grupo empresarial garantiza que sus políticas y lineamientos estén alineados con las mejores prácticas de la industria y con las obligaciones legales vigentes, lo que contribuye a fortalecer la protección de sus activos de información y ciberactivos frente a las amenazas en constante evolución.

Política de Ciberseguridad:

La política de ciberseguridad del grupo empresarial es un documento de alto nivel que refleja el compromiso de la alta dirección con la seguridad de la información y de las operaciones. Esta política establece el marco de actuación que guía las pautas de comportamiento de los colaboradores y terceros involucrados en el manejo de la información y de las tecnologías habilitadoras del negocio. Cada compañía del grupo empresarial tiene su propia política de ciberseguridad, derivada de la política corporativa, con el objetivo de establecer directrices específicas adaptadas a sus necesidades operativas y de seguridad.

La Política de Ciberseguridad del Grupo Empresarial Argos establece directrices y responsabilidades para proteger los activos de información y ciber activos de la compañía, garantizando su confidencialidad, integridad y disponibilidad de la información y de las tecnologías de la información para asegurar la sostenibilidad del negocio y la seguridad de las personas.

El objetivo de la política es establecer marcos y guías para el comportamiento de colaboradores y terceros en el manejo de información y tecnologías, garantizando la ciberseguridad de la compañía. Esta política aplica a todas las operaciones de la compañía y es de cumplimiento obligatorio para todos los colaboradores y terceros relacionados con las tecnologías de información y operación.

El Grupo Empresarial Argos se compromete a cumplir con leyes y regulaciones, gestionar riesgos y adoptar mejores prácticas en ciberseguridad para asegurar la sostenibilidad del negocio y la seguridad de las personas. Colaboradores y terceros deben asegurar que la política esté alineada con los objetivos de la compañía, apoyar activamente la ciberseguridad y adoptar un enfoque basado en la gestión de riesgos.

La información almacenada, creada o transmitida debe ser utilizada exclusivamente para los propósitos del negocio, manteniendo un inventario actualizado de los activos de información. Se deben establecer controles para prevenir la pérdida, daño, robo o mal funcionamiento de los activos de información, asegurando su confidencialidad, integridad y disponibilidad.

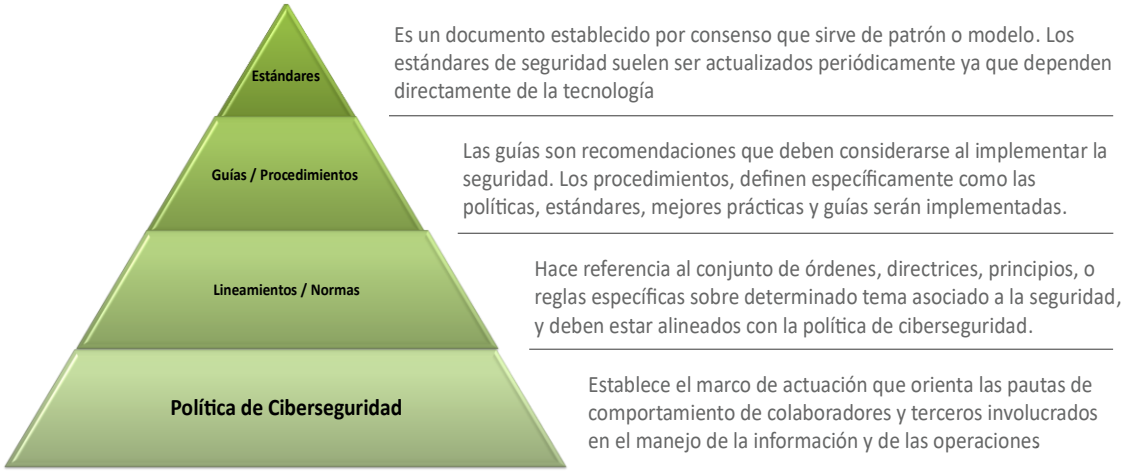
El Grupo Empresarial Argos ha definido una estructura organizacional con roles y responsabilidades específicas para asegurar el cumplimiento de la política de ciberseguridad. La política debe ser revisada anualmente o cuando sea necesario, y es aprobada por el Comité Estratégico de Ciberseguridad.

Lineamientos / Normas:

Los lineamientos y normas en materia de ciberseguridad establecen el conjunto de órdenes, directrices, principios y reglas específicas que deben seguirse para garantizar la seguridad de la información y de las operaciones. Estos lineamientos están alineados con la política de ciberseguridad del grupo empresarial y aseguran el cumplimiento de los objetivos y obligaciones legales. Cada compañía del grupo se compromete a implementar estos lineamientos y normas de manera coherente y efectiva, adaptándolos a su contexto operativo particular.

Anexos Técnicos / Guías:

Los anexos técnicos / Guías proporcionan documentación detallada y específica en forma de guías, procedimientos y estándares para la implementación de las políticas de ciberseguridad. Estos documentos abordan aspectos clave de la seguridad de la información, como la clasificación de activos, la seguridad en las operaciones, el uso seguro de recursos informáticos, la protección de datos y más. Cada anexo técnico / Guía proporciona orientación práctica para garantizar la aplicación efectiva de las políticas y lineamientos de ciberseguridad en las diferentes áreas y procesos de las compañías del grupo.



8. Gestión de Riesgos en Ciberseguridad

La gestión de riesgos en ciberseguridad es un componente fundamental de la estrategia de seguridad de la información del Grupo Empresarial. Se basa en una metodología estructurada que abarca la identificación, análisis, tratamiento y monitoreo continuo de los riesgos relacionados con la seguridad digital. Este proceso se desarrolla en varias etapas:

Identificación del Riesgo: Se lleva a cabo una exhaustiva identificación de los riesgos, considerando el objetivo, alcance y contexto del proceso o proyecto. Se identifican las amenazas, vulnerabilidades y posibles consecuencias, utilizando preguntas guía como: ¿Qué es lo que queremos proteger? (activo), ¿De qué lo debemos proteger? (amenaza), ¿Por qué puede materializarse la amenaza? (vulnerabilidad). Este proceso se apoya en herramientas como entrevistas, análisis documental, revisión de prácticas de la industria y tendencias globales. Los riesgos se clasifican en eventos internos, controlables por la organización, y eventos externos, fuera de su control directo. Este proceso sigue un enfoque estructurado que incluye: Identificar riesgos específicos (Riesgo 1, Riesgo 2, ..., Riesgo N), definidos como el efecto de la incertidumbre sobre la consecución de los objetivos de la Ciberseguridad. Para cada riesgo, se identifican las amenazas o causas

(acciones dañinas con consecuencias negativas), como Amenaza 1, Amenaza 2, ..., Amenaza N. Se determinan las vulnerabilidades asociadas (debilidades que facilitan la materialización de una amenaza), como Vulnerabilidad 1, Vulnerabilidad 2, etc. Se evalúan los controles existentes (Control 1, Control 2, ..., Control N) que mitigan las vulnerabilidades.

Análisis y Evaluación de Riesgos: Esta etapa tiene como objetivo determinar el nivel de exposición al riesgo, considerando la probabilidad de ocurrencia y el impacto potencial. Se identifican los controles existentes y se evalúa su efectividad en la mitigación de riesgos mediante la pregunta: ¿Qué se hace actualmente para reducir el riesgo? El nivel de riesgo se calcula evaluando cómo influyen las consecuencias en la entidad (impacto) y cuál es la posibilidad de que ocurra (probabilidad). Los riesgos se califican según su nivel de exposición y se ubican en un mapa de riesgos, que facilita la priorización de acciones.

Tratamiento del Riesgo: Después de analizar la exposición al riesgo, se definen planes de acción para mitigar los riesgos críticos, altos o moderados. Se evalúan diferentes opciones de tratamiento, como evitar, mitigar, transferir o retener el riesgo, basadas en criterios de costo/beneficio y mitigación esperada.

Monitoreo: Se establecen mecanismos de monitoreo y reporte continuo para una gestión de riesgos efectiva. Se realiza seguimiento a la implementación de planes de acción y se revisan periódicamente los análisis de riesgos para garantizar su vigencia. El reporte de riesgos se consolida para informar a los grupos de interés relevantes dentro de la organización.

Nivel de exposición = probabilidad x impacto

Probabilidad						
	5 Muy Alta	5	10	20	40	80
	4 Alta	4	8	16	32	64
	3 Moderada	3	6	12	24	48
	2 Baja	2	4	8	16	32
	1 Muy Baja	1	2	4	8	16
Bajo Moderado Alto Crítico		1 Menor	2 Bajo	4 Importante	8 Mayor	16 Significativo
		Impacto				

El mapa de riesgos está dividido en cuatro zonas de riesgo: bajo, moderado, alto y crítico.

Riesgos de Ciberseguridad Identificados

Los riesgos específicos en el ámbito de la ciberseguridad se evalúan y gestionan según la metodología establecida. Algunos de estos riesgos incluyen:

Pérdida de Confidencialidad y Divulgación No Autorizada de la Información: Puede ser causada por espionaje industrial, fuga o robo de información, o pérdida de equipos.

Alteración y Modificación No Autorizada de la Información o Sistemas: La integridad de la información puede comprometerse por la introducción de malware, virus o ransomware.

Pérdida, Destrucción o Indisponibilidad de la Información: Los datos pueden estar en riesgo de pérdida, destrucción o no estar disponibles cuando sea necesario.

Incumplimiento Normativo y/o Regulatorio: El tratamiento inadecuado de la información puede llevar a incumplimientos normativos o regulatorios, especialmente en lo relacionado con la privacidad de los datos.

CyberRisk: La indisponibilidad, interrupción o daño de los sistemas de información y operación debido a amenazas informáticas representa un riesgo significativo.

Engaños a Sistemas y Personas: Tecnologías emergentes como el data poisoning o deepfakes pueden utilizarse maliciosamente para engañar sistemas de información y personas.

Vulnerabilidades en Servicios Tecnológicos de Proveedores: Las vulnerabilidades en los servicios tecnológicos provistos por terceros que conforman la cadena de suministro de la compañía pueden exponer a la organización a riesgos de seguridad.

9. Sistema de Gestión Integral de Ciberseguridad (Framework)

El sistema de gestión de ciberseguridad del Grupo Empresarial se basa en frameworks reconocidos como NIST, COBIT e ISO 27000, así como estándares específicos de las industrias atendidas, incluyendo NERC CIP (energía), ISA99 (manufactura), RAC 160 (aeronáutica), y regulaciones financieras como GDPR y SEC. Este sistema integra mejores prácticas de ciberseguridad, alineándose con el gobierno corporativo, las estrategias de negocio, la gestión de riesgos de cada compañía, y los requisitos de socios estratégicos en cada sector. Este programa integra las mejores prácticas de ciberseguridad y se nutre del gobierno corporativo de cada una de las compañías, sus estrategias de negocio y gestión de riesgos, así como de los lineamientos específicos de sus socios estratégicos en cada sector industrial. En 2025, el sistema adopta un enfoque de *Zero Trust* para unificar controles en entornos híbridos, incorpora gobernabilidad ética de la IA para proteger contra amenazas como data poisoning y deepfakes, y prepara la infraestructura para computación cuántica con criptografía poscuántica. Esto permite al grupo ofrecer servicios de ciberseguridad a terceros, fortaleciendo su posición competitiva.

En el sector de inversiones financieras, se aplican normativas como GDPR (Reglamento General de Protección de Datos) en Europa y regulaciones específicas de la SEC (Comisión de Valores y Bolsa de Estados Unidos) en Estados Unidos. En el sector de energía, se cumplen normativas como NERC CIP (Normas de Protección de la Infraestructura Crítica) y regulaciones específicas del mercado energético en cada país donde opera el

grupo empresarial, reforzando la protección de sistemas OT contra ataques que buscan daños físicos. En manufactura, se implementan estándares ISA99 y soluciones para mapear dispositivos IoT/OT, mitigando riesgos en la cadena de suministro. En concesiones viales y aeroportuarias, se cumplen regulaciones de seguridad y privacidad de datos establecidas por organismos gubernamentales como la OAS (Organización de los Estados Americanos) y agencias de control de la aviación como la FAA (Administración Federal de Aviación). Este enfoque integral garantiza que el programa de gestión de ciberseguridad está alineado con las normativas y regulaciones específicas de cada industria, asegurando así la protección adecuada de los activos de información y la mitigación de riesgos cibernéticos en todas las operaciones del Grupo Empresarial.

El sistema de gestión de ciberseguridad se basa en un ciclo de mejora continua PHVA en cada una de sus 7 funciones:

Gobierno: Fortalecimiento del gobierno de ciberseguridad para identificación, evaluación y reducción del riesgo de ciberseguridad. Incluye la definición de comités estratégicos y tácticos de gestión, así como la elaboración de políticas de ciberseguridad.

Identificación: Identificación de activos críticos de información, evaluación de amenazas y reevaluación del riesgo cibernético.

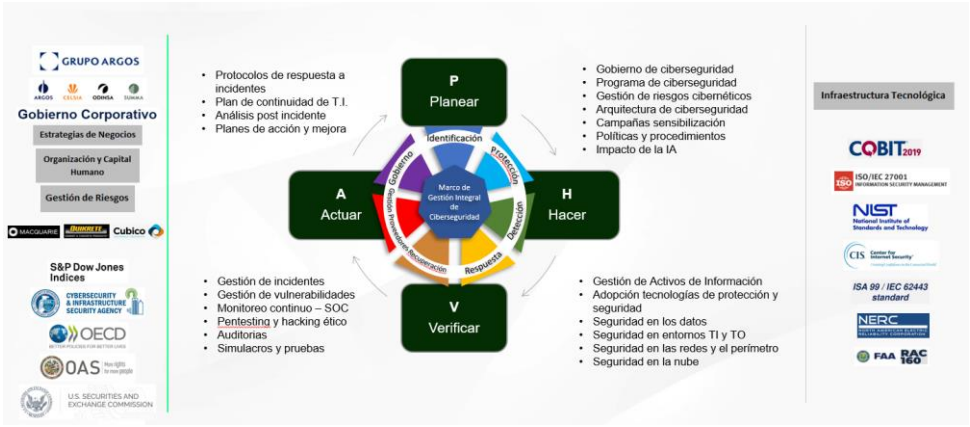
Protección: Desarrollo de capacidades para proteger los activos de información contra amenazas cibernéticas. Incluye la adopción de tecnologías y medidas preventivas.

Detección: Implementación de herramientas y procesos para la detección temprana de amenazas cibernéticas y actividades maliciosas.

Respuesta: Desarrollo de planes de respuesta a incidentes de seguridad para responder oportuna y eficazmente a los ataques cibernéticos.

Recuperación: Planificación de la continuidad operativa y recuperación de la información en caso de materialización de un ataque cibernético.

Gestión de Terceras Partes: Integración de políticas y controles de ciberseguridad en la cadena de suministro y colaboración con terceros proveedores.



10. Estrategia de Ciberseguridad

1. Perspectivas

Para adaptarse a las tendencias y desafíos emergentes en ciberseguridad, nuestra estrategia considera las siguientes perspectivas clave:

Inteligencia Artificial y Aprendizaje Automático: Se espera un mayor uso de estas tecnologías para identificar y detectar amenazas de manera más rápida y precisa, provechando la IA y el aprendizaje automático para mejorar la detección y respuesta a amenazas avanzadas, como deepfakes y phishing impulsado por IA e integrando una gobernabilidad ética de la IA para prevenir riesgos como data poisoning y sesgos algorítmicos, permiten al grupo ofrecer servicios de ciberseguridad gestionada basados en IA a clientes externos.

Protección de la Privacidad: Enfoque renovado en la protección de la privacidad de los datos y control de la información personal, por lo que reforzar la privacidad de los datos mediante un marcos de Zero Trust que garanticen autenticación continua y controles granulares, cumpliendo normativas globales (GDPR) e Implementar soluciones de gestión de identidades para proteger datos sensibles en entornos híbridos, posicionan al grupo como proveedor confiable de servicios de privacidad para terceros.

Internet de las Cosas (IoT): La seguridad en entornos IoT y OT se ha convertido en una prioridad clave ante el aumento de dispositivos conectados y su exposición a ciberataques. Es fundamental proteger estos activos para evitar brechas de seguridad y daños físicos, especialmente en sectores como manufactura y energía. Esto exige mapear y monitorear dispositivos en entornos dispersos, así como ofrecer servicios especializados de seguridad IoT/OT que garanticen visibilidad, control y respuesta efectiva ante amenazas.

Ransomware y Ataques de Rescate: El ransomware sigue siendo una de las amenazas más críticas, especialmente en sus variantes de doble y triple extorsión, que combinan cifrado, robo y divulgación de datos. La estrategia de ciberseguridad debe enfocarse en la prevención y respuesta efectiva, incluyendo capacidades para detectar ataques dirigidos a entornos OT que eliminan rastros forenses. Fortalecer las defensas, mantener respaldos seguros y contar con planes de respuesta robustos son esenciales para mitigar el impacto de estos ataques cada vez más sofisticados.

Ciberseguridad en la Nube: La ciberseguridad en la nube es esencial ante la creciente adopción de entornos híbridos. Es clave desarrollar soluciones sólidas que protejan los datos y servicios, integrando herramientas de detección para mitigar configuraciones erróneas y ataques a APIs. La implementación de modelos como Zero Trust Network Access (ZTNA) refuerza el control de acceso y la segmentación. Además, se busca posicionar al grupo como proveedor de servicios de seguridad en la nube para terceros, aprovechando su experiencia y la demanda del mercado.

Amenazas a la Inteligencia Artificial: La protección de sistemas de Inteligencia Artificial se vuelve crucial ante amenazas emergentes como el prompt injection y el data poisoning, que buscan manipular modelos de machine learning. Es fundamental implementar auditorías éticas, controles de acceso estrictos y mecanismos

de validación de datos para salvaguardar la integridad de estos sistemas. La ciberseguridad debe adaptarse para garantizar que la IA opere de forma segura, confiable y alineada con los objetivos de las compañías.

Preparación para la Computación Cuántica: La preparación para la era de la computación cuántica exige priorizar la transición hacia criptografía poscuántica (PQC) para proteger datos sensibles ante futuros ataques. Siguiendo las directrices del NIST y los plazos establecidos por el DHS para 2030 en sistemas críticos, es vital comenzar la evaluación y adopción de algoritmos resistentes a la computación cuántica, asegurando así la resiliencia a largo plazo de la información estratégica.

Resiliencia Frente a Amenazas a Sistemas Industriales (OT): Proteger sistemas OT contra ataques que buscan daños físicos, como los identificados por el SANS Institute, usando segmentación y monitoreo en tiempo real. Esto permite al grupo ofrecer soluciones de seguridad OT a industrias externas, como energía o manufactura, diversificando su portafolio.

2. Premisas para la Construcción de la Estrategia

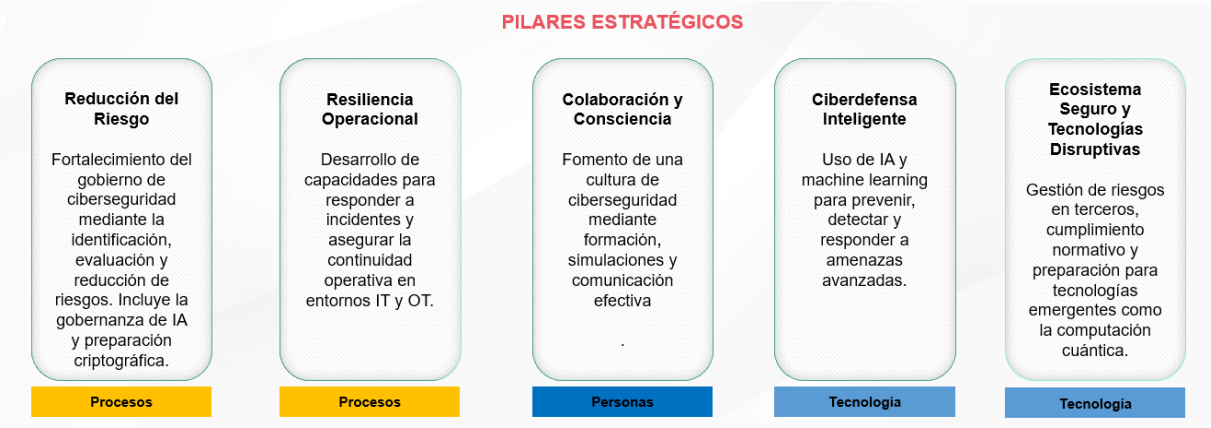
El foco principal de la estrategia actual de ciberseguridad es construir un ecosistema de ciberseguridad resiliente y ético basado en Zero Trust, que integre la gobernabilidad de la IA, la preparación para la computación cuántica, y la seguridad del ecosistema de terceros, para proteger las operaciones globales del grupo empresarial y posicionarlo como un proveedor líder de servicios de ciberseguridad en mercados externos. Este enfoque responde a las amenazas avanzadas, como el aumento del 1,000% en phishing impulsado por IA, deepfakes, ataques a sistemas OT que buscan daños físicos y la necesidad de proteger la cadena de suministro con Software Bill of Materials (SBOM).

El fortalecimiento del sistema de gestión promueve una cultura ética mediante formación en amenazas emergentes y auditorías de IA. La nueva premisa sobre el ecosistema de terceros asegura la colaboración segura con proveedores y socios mediante controles Zero Trust e inteligencia de amenazas global, mitigando riesgos en entornos dispersos. Esta estrategia no solo protege las operaciones globales del grupo, sino que lo consolida como líder en ciberseguridad, capaz de expandir servicios a clientes externos, con o sin participación accionaria, en un mercado cada vez más exigente.

3. Estrategia de Ciberseguridad

La estrategia de ciberseguridad del Grupo Empresarial se fundamenta en el propósito superior de mantener la confianza y seguridad digital de nuestros clientes y usuarios, con el objetivo específico de proteger los activos y datos críticos de la organización contra amenazas cibernéticas, se basa en una estrategia integral que abarca la reducción del riesgo, la resiliencia, la colaboración y la consciencia, así como la implementación de medidas de ciberdefensa. Se apoya en frameworks reconocidos y se nutre del gobierno corporativo, las estrategias de negocio y las agencias de gobierno y control para garantizar la confianza y seguridad digital en la organización.

Esta estrategia se estructura en cinco pilares fundamentales:



Pilar 1: Reducción del Riesgo

Este pilar se enfoca en fortalecer el gobierno de ciberseguridad para identificar, evaluar y reducir el riesgo de ciberseguridad. Se establecen capacidades sólidas de identificación de riesgos y se consolida un gobierno de ciberseguridad mediante la definición de comités estratégicos y tácticos de gestión. También se establecen políticas de ciberseguridad que enmarcan la postura de la organización en la protección de los activos de información. Este pilar incluye la identificación de activos de información y ciberactivos, la evaluación de amenazas y la reevaluación del riesgo cibernético.

Este pilar incluye:

Fortalecimiento del gobierno de ciberseguridad para identificación, evaluación y reducción del riesgo.

Definición de comités estratégicos y tácticos de gestión.

Elaboración de políticas de ciberseguridad que enmarquen la postura de las compañías en la protección de los activos de información.

Implementar un marco de gobernabilidad ética de la IA para auditar modelos y prevenir riesgos como data poisoning, sesgos o cualquier amenaza a la información.

Realizar inventarios criptográficos para identificar sistemas vulnerables a amenazas cuánticas.

Pilar 2: Resiliencia

La resiliencia se refiere a la capacidad de la organización para responder de manera oportuna y eficaz a los ataques cibernéticos y garantizar la continuidad operativa. En este pilar se desarrollan planes de respuesta a incidentes de seguridad y planes de continuidad que permiten a la organización enfrentar y recuperarse rápidamente de los ciberataques.

Este pilar incluye:

Desarrollo de capacidades para responder y asegurar la continuidad operativa ante ataques cibernéticos, incluyendo el diseño de planes de continuidad que integren IT y OT para ataques a infraestructuras críticas.

Elaboración de planes de respuesta a incidentes de seguridad y planes de continuidad.

Pilar 3: Colaboración y Consciencia

Este pilar se centra en fomentar la cultura de ciberseguridad y promover la colaboración entre diferentes partes interesadas, tanto internas como externas. Se establecen canales de comunicación efectivos y se promueve la pedagogía en materia de ciberseguridad. La conciencia y la colaboración son fundamentales para fortalecer las defensas y hacer frente a las amenazas cibernéticas de manera conjunta.

Este pilar incluye:

Fomento de la cultura de ciberseguridad y colaboración entre diferentes partes interesadas, tanto internas como externas, incluyendo programas de formación sobre deepfakes, phishing IA, y uso ético de IA, adaptados a las industrias del grupo.

Integrar simulaciones de amenazas (phishing, ataques OT) para reforzar la consciencia en empleados y socios.

Implementación de canales de comunicación efectivos y programas de pedagogía en ciberseguridad.

Pilar 4: Ciberdefensa

El pilar de ciberdefensa se enfoca en adoptar tecnologías y herramientas de protección de la ciberseguridad, incluyendo capacidades de machine learning e inteligencia artificial (IA) para hacer frente a las amenazas emergentes con eficiencia. La inteligencia artificial generativa ha desempeñado un papel crucial, no solo en manos de los cibercriminales, sino también en la aceleración de la detección de ciberataques a nivel mundial. Se destaca la utilidad de la inteligencia artificial en analizar grandes volúmenes de datos y mejorar la detección de amenazas. En un contexto geopolítico, la ciberguerra y el hacktivismo son cada vez más relevantes, lo que hace necesario contar con políticas preventivas, detectivas y correctivas, así como herramientas de ciberseguridad actualizadas.

Este pilar incluye:

Adopción de tecnologías para la protección de la ciberseguridad, incluyendo capacidades de machine learning e IA para enfrentar amenazas emergentes.

Implementación de acciones y políticas preventivas, detectivas y correctivas para proteger los sistemas informáticos y los datos.

Pilar 5: Integración Estratégica del Ecosistema de Terceros y Tecnologías Disruptivas

Asegurar la seguridad, interoperabilidad y resiliencia del ecosistema de terceros (proveedores, socios estratégicos, cadenas de suministro) del grupo empresarial, mientras se lidera en la adopción de tecnologías disruptivas, posicionando al grupo empresarial como innovador global.

Este pilar incluye:

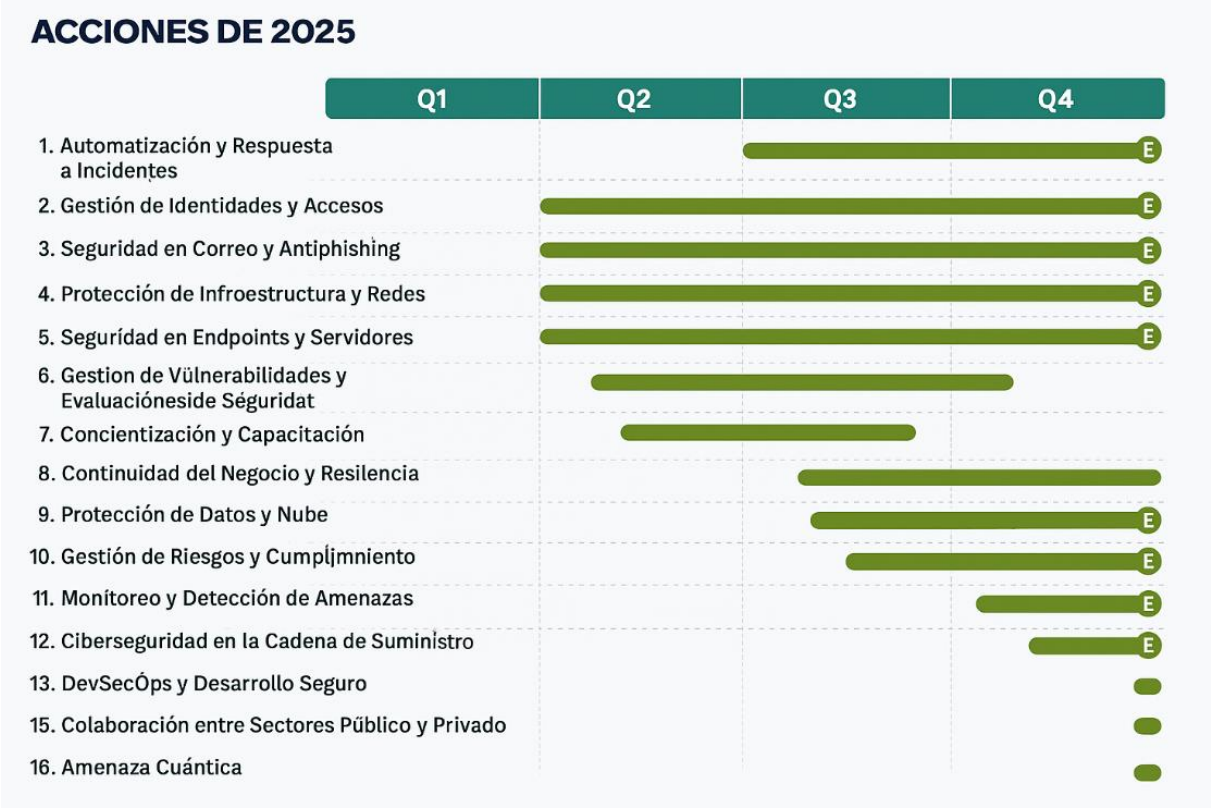
Fortalecer la seguridad de terceros mitigando riesgos en Manufactura y Energía

Integrar inteligencia de amenazas para monitorear actores en la dark web, asegurando la confianza de socios e inversionistas.

Preparar la infraestructura para computación cuántica

Alinear con normativas (NERC CIP, ISA99, GDPR, FAA) para garantizar interoperabilidad con socios externos.

Ofrecer servicios de auditoría de ecosistemas y soluciones de seguridad



11. Arquitectura y Controles de Ciberseguridad

La Arquitectura de Ciberseguridad se define como un conjunto de representaciones que describen la función, estructura e interrelación de los componentes de seguridad dentro de nuestro entorno de Tecnologías de la Información y Operación. Nuestra arquitectura se basa en principios fundamentales. En primer lugar, aplicamos el concepto de Seguridad por Diseño, garantizando que la protección de la información esté alineada con los objetivos del negocio y considerando la interconectividad e interoperabilidad de los sistemas. Asimismo, se implementa la Autorización por menor Privilegio, asegurando que tanto personas, sistemas, aplicaciones y procesos tengan acceso solo a la información necesaria para cumplir con sus funciones, estableciendo como estado predefinido el de no acceso. Buscamos la Estandarización de nuestros componentes de seguridad para reducir la complejidad y el costo de la seguridad, garantizando procesos uniformes y facilitando la automatización. Además, se implementa el principio de Defensa en Profundidad, que consiste en asegurar una protección integrada y activar controles en todas las capas del sistema. Este principio, detallado más adelante en este documento, es fundamental para garantizar una seguridad robusta y adaptable a las distintas amenazas. Consideramos la redundancia de los sistemas para mitigar posibles fallas de seguridad y garantizar la continuidad del negocio. Nos esforzamos por lograr la Aceptación por parte de los usuarios, asegurando que nuestras medidas de seguridad sean psicológicamente aceptables. Adicionalmente, aplicamos el Principio de la Identidad, asegurando que todos los componentes de seguridad tengan un identificador único. Por último, gestionamos los riesgos de manera efectiva para reducir la exposición a la información y maximizar el rendimiento de nuestras Tecnologías de la Información y Operación.

El principio de defensa en profundidad es una estrategia fundamental en ciberseguridad que busca proporcionar una serie de capas de seguridad superpuestas y complementarias para proteger los activos de información y sistemas del grupo empresarial. Esta estrategia se basa en la idea de que, si una capa de seguridad falla o es vulnerada, otras capas adicionales están en su lugar para prevenir, detectar o mitigar posibles ataques o intrusiones.

En lugar de depender únicamente de una sola medida de seguridad, se implementan múltiples capas de seguridad con diferentes enfoques y controles, lo que aumenta significativamente la robustez del sistema de seguridad. Algunas de las capas de seguridad que se pueden implementar como parte de la defensa en profundidad incluyen:

Perímetro de red: Utilizamos firewalls, sistemas de prevención de intrusiones (IPS), sistemas de detección de intrusiones (IDS) y otros dispositivos de seguridad para proteger el perímetro de la red y controlar el tráfico entrante y saliente.

Identidades, Autenticación y control de acceso: Se implementan medidas como contraseñas seguras, autenticación multifactor (MFA), controles de acceso basados en roles (RBAC) y políticas de acceso para garantizar que solo los usuarios autorizados tengan acceso a los sistemas y datos. Además, nos enfocamos en la gestión de identidades, que abarca la administración centralizada y segura de las identidades digitales de los usuarios, incluyendo la creación, modificación, desactivación y eliminación de cuentas de usuario de

manera oportuna y controlada. A través de un enfoque integral de seguridad en las identidades, fortalecemos nuestra capacidad para proteger nuestros activos de información y prevenir el acceso no autorizado a nuestros sistemas y datos sensibles.

Seguridad en el endpoint: Se implementan medidas de seguridad en los dispositivos finales, como computadoras y dispositivos móviles, para protegerlos contra amenazas como malware, ransomware y ataques de phishing.

Seguridad de aplicaciones: Se implementan controles de seguridad en el desarrollo de aplicaciones, como pruebas de penetración, análisis estático y dinámico de código, y firewalls de aplicaciones web (WAF), para proteger las aplicaciones contra vulnerabilidades y ataques.

Seguridad de los datos: Se implementan medidas de cifrado, tanto en tránsito como en reposo, para proteger la confidencialidad y la integridad de los datos. También Se implementan controles de prevención de pérdida de datos (DLP) y mecanismos de respaldo y recuperación para garantizar la disponibilidad de los datos.

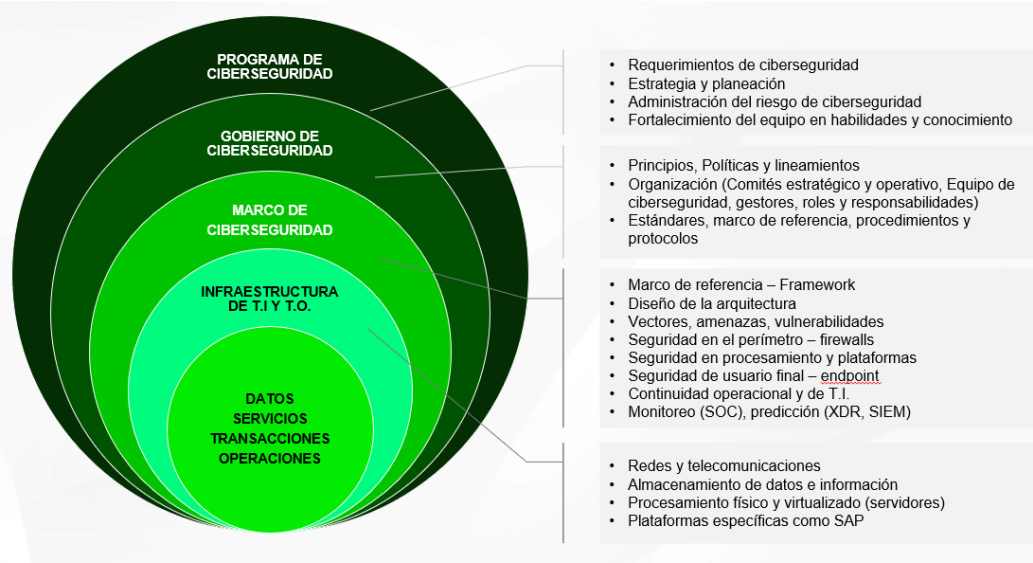
Seguridad en la nube: Se implementan medidas de seguridad específicas para proteger los datos y los sistemas que residen en entornos de nube pública, privada o híbrida. Esto incluye el uso de servicios de seguridad en la nube, como firewalls de aplicación web (WAF), controles de acceso basados en políticas, cifrado de datos y monitoreo continuo de la seguridad en la nube.

Seguridad en los sistemas industriales (TO): Aseguramos la integridad y disponibilidad de los sistemas industriales y de operación (TO) mediante la implementación de controles de seguridad específicos, como segmentación de red, monitoreo de activos críticos y actualizaciones regulares de seguridad.

Seguridad en el desarrollo de software: Integramos medidas de seguridad en todo el ciclo de vida del desarrollo de software, incluyendo pruebas de penetración, análisis estático y dinámico de código, y capacitación en seguridad para desarrolladores, con el fin de prevenir vulnerabilidades y asegurar la seguridad de las aplicaciones.

Detección y respuesta de intrusiones: Utilizamos herramientas y sistemas para monitorear y detectar actividad maliciosa o sospechosa en la red y los sistemas. Esto puede incluir sistemas de detección de intrusiones (IDS), sistemas de información y eventos de seguridad (SIEM) y análisis de comportamiento de usuarios y entidades (UEBA).

Concientización y capacitación: Realizamos programas de concientización y capacitación en seguridad cibernética para educar a los empleados sobre las mejores prácticas de seguridad y promover una cultura de seguridad en la organización.



Al implementar la defensa en profundidad en todas estas áreas, fortalecemos nuestra postura de seguridad cibernética y reducimos significativamente la probabilidad de sufrir ataques exitosos. Cada capa de seguridad contribuye a la protección global de los activos de información y sistemas, creando un entorno de seguridad más resistente y adaptable a las amenazas en constante evolución.

12. Gestión de Vulnerabilidades Tecnológicas

La gestión de vulnerabilidades es un componente esencial dentro del programa de ciberseguridad del Grupo Empresarial, diseñada para mitigar los riesgos derivados de las brechas de seguridad presentes en las plataformas tecnológicas. Este proceso parte de la identificación de vulnerabilidades mediante un enfoque agnóstico y multidimensional, que considera recursos humanos, escaneos automatizados, auditorías técnicas

y herramientas especializadas. El objetivo es comprender los riesgos reales que afectan los activos críticos y ofrecer soluciones efectivas para cerrarlos, con un alcance que cubre todos los sistemas tecnológicos del grupo. El proceso comienza con la identificación de los sistemas a evaluar y culmina con la remediación confirmada de las vulnerabilidades y la emisión del informe de cierre. Véase: Procedimiento de gestión de vulnerabilidades

Lineamientos

El procedimiento establece lineamientos que permiten detectar, evaluar y tratar de forma constante las debilidades de seguridad en los activos tecnológicos. La gestión inicia con el reporte de activos críticos por parte del área de Infraestructura, seguido por la toma de muestra y su inclusión en la herramienta de escaneo. Las pruebas se realizan de forma continua para sistemas con agentes instalados y mensualmente para los demás. Los resultados son gestionados por el equipo de Ciberseguridad, en colaboración con el Centro de Operaciones de Seguridad (SOC), sin afectar la operatividad de los procesos de negocio. Las vulnerabilidades detectadas se clasifican según su criticidad (crítica, alta, media, baja), lo que determina el tiempo máximo recomendado para su tratamiento, desde un mes para las críticas, hasta seis meses para las bajas.

Los plazos establecidos para la remediación varían según la criticidad del hallazgo. Las vulnerabilidades críticas deben contar con controles compensatorios en los primeros siete días y cerrarse completamente en el plazo de un mes. Las vulnerabilidades altas tienen un plazo de dos meses, las medias tres y las bajas seis. Las excepciones a estos plazos solo pueden ser aprobadas por el CISO, considerando factores como el nivel de exposición del activo, su valor estratégico y su historial como objetivo de ataques.

Roles y Responsabilidades

El proceso cuenta con una distribución clara de responsabilidades. El Especialista de Ciberseguridad se encarga de documentar, analizar e implementar mejoras en el ciclo de vida de las vulnerabilidades. El Gestor de Ciberseguridad lidera la implementación de controles técnicos y asegura el cumplimiento de políticas, además de generar los informes y métricas requeridas. El CISO, por su parte, es responsable de la toma de decisiones estratégicas, como la aprobación de excepciones y la elección de herramientas. Los especialistas de redes, infraestructura, aplicaciones e informática de usuarios son responsables de aplicar los parches, gestionar configuraciones y entregar soportes de aceptación de riesgos cuando no se puedan mitigar ciertas vulnerabilidades.

Flujo del proceso y gestión de hallazgos

El flujo del proceso operativo inicia con la verificación de activos tecnológicos a escanear, su correcta configuración en la herramienta de escaneo y la ejecución de la prueba. Una vez se obtienen los resultados, se realiza un análisis detallado que clasifica los hallazgos y permite validar si se requiere acción inmediata. En casos críticos, se activa el proceso de cambio para aplicar parches de emergencia. Para vulnerabilidades de menor criticidad, se documenta una matriz de vulnerabilidades que luego es divulgada a los equipos

responsables. Estos equipos deben implementar acciones de corrección, las cuales son gestionadas y validadas por la célula de trabajo encargada del ciclo de vida de vulnerabilidades.

El proceso también contempla la gestión de hallazgos provenientes de pruebas de Ethical Hacking (ETH), las cuales permiten identificar debilidades explotables de forma más profunda. Estos hallazgos son analizados para determinar si requieren acciones inmediatas y, si es así, se gestiona el cambio de emergencia correspondiente. En todos los casos, se realiza un seguimiento riguroso a las recomendaciones hasta confirmar el cierre de las brechas. Finalmente, se elaboran informes detallados con los resultados de cada ejercicio, que sirven como evidencia para las áreas responsables y como insumo para futuras auditorías.

El proceso cuenta con documentación de apoyo como diagramas de flujo y una línea base de activos críticos. Además, se manejan conceptos clave para la comprensión del proceso, tales como vulnerabilidad, riesgo, escaneo, activos críticos y pruebas de hacking ético. Estos elementos permiten un entendimiento común entre los actores involucrados y fortalecen la gobernanza del proceso.

13. Gestión de la Continuidad de Negocio

La gestión de la continuidad del negocio es un pilar estratégico que fortalece la resiliencia del Grupo Empresarial, proporcionando un marco sólido basado en políticas, lineamientos, análisis de impacto, estrategias, procedimientos y roles bien definidos. Este programa prepara a la organización para enfrentar interrupciones—como fallos técnicos o ataques cibernéticos—, emergencias que afecten instalaciones físicas, y crisis de alto impacto reputacional, asegurando la operación continua de procesos críticos en Manufactura, Energía, Concesiones e Inversiones Financieras. Más allá de proteger los intereses del grupo, esta iniciativa fomenta una cultura de preparación y respuesta entre los colaboradores, eleva la reputación institucional y posiciona al grupo como un líder competitivo, capaz de ofrecer soluciones de continuidad a terceros en un entorno global.

El modelo de continuidad se estructura en tres ejes clave: interrupciones (fallos técnicos, errores humanos o actos maliciosos, incluidos ataques a sistemas operativos), emergencias (eventos que comprometan la infraestructura física), y crisis (escenarios prolongados con repercusiones reputacionales). Este enfoque, respaldado por estándares internacionales y tecnologías emergentes como la criptografía avanzada, asegura que el grupo no solo supere disrupciones, sino que las transforme en oportunidades, integrando la ciberseguridad como un componente esencial de su estrategia.

El propósito central del programa es establecer un marco estratégico y operativo que garantice la continuidad del negocio del Grupo Empresarial frente a eventos disruptivos, alineándose con estándares globales reconocidos. Este marco busca prevenir, contener y recuperar operaciones de manera eficiente, protegiendo la confidencialidad, integridad y disponibilidad de la información. En 2025, el programa se enfoca en anticipar amenazas emergentes como ataques a sistemas críticos y riesgos tecnológicos avanzados, mientras fortalece

la capacidad del grupo para ofrecer servicios de continuidad a clientes externos, consolidando su liderazgo en sectores regulados como Energía y Concesiones.

El programa abarca todas las empresas del Grupo Empresarial, sus procesos críticos, servicios de tecnología, infraestructura física y digital, colaboradores, y terceros estratégicos, incluyendo proveedores y socios en Manufactura, Energía, Concesiones e Inversiones Financieras. En 2025, su alcance se extiende a ecosistemas externos, apoyando la expansión comercial con soluciones de ciberseguridad gestionada.

Componentes Clave del Programa

El programa descansa en tres componentes interdependientes que aseguran una respuesta integral. Prevención protege la vida, el bienestar y los recursos críticos, reduciendo la probabilidad de interrupciones mediante controles predictivos y auditorías de terceros. Contención habilita una respuesta rápida y efectiva ante incidentes, minimizando impactos con planes integrales para sistemas tecnológicos y operativos. Recuperación restaura procesos críticos basándose en análisis de impacto (BIA) y métricas como tiempo de recuperación (RTO) y punto de recuperación (RPO), integrando soluciones avanzadas para enfrentar amenazas tecnológicas, y ofreciendo servicios de recuperación a terceros como aeropuertos o plantas energéticas.

Gobierno de Continuidad

El programa establece una estructura organizacional estratégica y clara. Las Juntas Directivas y Comités de Auditoría, Finanzas y Riesgos lideran la aprobación, supervisión y seguimiento, asegurando alineación con los objetivos corporativos. Los presidentes de compañías del grupo empresarial y Comités Directivos impulsan la implementación y reportan avances, mientras el Área de Gestión Integral de Riesgos diseña políticas y lidera la estrategia. Las Áreas de Riesgo y Tecnología de las filiales ejecutan tácticas operativas, y los dueños de Procesos y Gestores de Riesgos identifican riesgos y promueven una cultura de continuidad. Auditoría Interna evalúa la efectividad, y todos los empleados aplican los protocolos, apoyando la expansión de servicios de continuidad a terceros.

Planes de Respuesta Relacionados

La continuidad del negocio se articula a través de planes integrales que garantizan una respuesta adaptativa. Los Planes de Emergencia de SUMMA abordan emergencias físicas en sedes administrativas, protegiendo la infraestructura crítica. El Plan de Manejo de Crisis (PMC) equipa al Comité de Manejo de Crisis (CMC) con herramientas para gestionar escenarios de alto impacto, adaptándose a eventos como ciberataques prolongados. El Plan de Recuperación de Tecnología (DRP) restaura plataformas tecnológicas críticas con simulaciones y soluciones avanzadas, mientras los Procedimientos de Recuperación de Procesos Críticos (BCP) restauran operaciones esenciales en Manufactura, Energía y Concesiones, ofreciendo servicios a terceros como aeropuertos.

Integración con Ciberseguridad

El Programa de Continuidad se integra de manera estratégica con el Programa de Ciberseguridad, reconociendo que incidentes como ransomware, intrusiones o ataques a sistemas operativos son causas principales de disrupciones. El Procedimiento de Atención de Incidentes de Ciberseguridad, apoyado por tecnologías predictivas y segmentación, asegura detección, análisis, contención y erradicación de amenazas, facilitando la restauración segura de servicios tecnológicos. Esta coordinación garantiza una respuesta rápida a ciberataques, activa planes de recuperación (DRP, BCP, PMC) de inmediato, y alinea al Comité de Crisis para incidentes escalados, priorizando procesos críticos definidos en el BIA.

Responsables de Control y Aprobación

El programa involucra a las Juntas Directivas, Comités de Auditoría, Finanzas y Riesgos, Presidencias de las compañías, Áreas de Riesgo y Tecnología, Gestores de Riesgos, Áreas de Auditoría Interna, y todos los empleados, quienes desempeñan un rol activo en su implementación y promoción, además de clientes externos que acceden a servicios relacionados.

Las Juntas Directivas aprueban el programa, mientras los Comités de Auditoría, Finanzas y Riesgos supervisan su ejecución y evolución, asegurando alineación con normativas y objetivos estratégicos, incluyendo la preparación para mercados globales.

14. Protección y Cifrado de Datos

El objetivo principal de esta sección es establecer criterios técnicos robustos para el cifrado de información, tanto en tránsito como en reposo, alineados con la clasificación de datos del Grupo Empresarial. Este enfoque protege la confidencialidad, integridad y disponibilidad de la información, fortaleciendo la seguridad y ciberseguridad en un entorno global y disperso. En 2025, el programa prioriza la anticipación a riesgos emergentes, como amenazas cuánticas y ataques avanzados, asegurando la protección de datos críticos en Manufactura, Energía, Concesiones e Inversiones Financieras, mientras se cumple con normativas como NERC CIP, GDPR, FAA e ISA99.

Enfoque Estratégico

La protección y el cifrado de datos son fundamentales para garantizar mecanismos de autenticación sólidos, la no repudiación, y la seguridad de la información y las identidades corporativas frente a amenazas cibernéticas. Este enfoque integral minimiza riesgos asociados a fugas de información confidencial, protegiendo los datos sensibles del grupo y de sus socios estratégicos en todas las industrias. Para ello, se implementan protocolos avanzados como TLS (Transport Layer Security) e IPSec (Internet Protocol Security), asegurando el transporte seguro de datos en redes internas y externas, incluyendo conexiones a internet. Estos protocolos se utilizan

para proteger información confidencial, como datos financieros o de infraestructura crítica, frente a accesos no autorizados.

El cifrado cumple con estándares internacionales, como los establecidos por NIST en el estándar FIPS, garantizando que los algoritmos y módulos utilizados sean resistentes a ataques de fuerza bruta, incluso por actores con capacidad computacional significativa. Esto aplica tanto a contraseñas de usuarios con bajos privilegios como a las de administradores, protegiendo sistemas críticos en Energía y Manufactura. Además, se prioriza la preparación para tecnologías disruptivas mediante la adopción de criptografía poscuántica (PQC), asegurando que los sistemas del grupo estén listos para resistir amenazas cuánticas futuras, especialmente en sectores regulados como Inversiones Financieras.

Actividades Clave

Para garantizar una protección efectiva, el programa establece actividades específicas. Las vulnerabilidades criptográficas críticas, como aquellas que puedan comprometer sistemas a gran escala, se remediaban en un plazo máximo de 60 días tras su identificación, implementando controles preventivos y de detección si la corrección total no es viable de inmediato. Las llaves de cifrado se almacenan de manera centralizada y segura por un período de hasta cinco años desde su último uso, facilitando investigaciones corporativas, legales o judiciales, un aspecto clave para Concesiones e Inversiones Financieras.

La información confidencial en reposo se protege mediante almacenamiento físico en locaciones seguras, como cajas fuertes, o mediante cifrado con llaves separadas de los datos encriptados, asegurando su integridad en todas las empresas del grupo. Además, se mantiene un registro detallado y separado de los datos cifrados, permitiendo a los investigadores validar que la información perdida estaba protegida al momento del incidente, un requisito crucial para cumplir normativas como GDPR. Los mecanismos de autenticación implementados son robustos, resistiendo ataques como keylogging, replay, secuestro de sesión y fuerza bruta, utilizando certificados digitales, contraseñas de único uso, autenticación multifactor, y cifrado simétrico y asimétrico, lo que refuerza la protección de identidades en todos los sectores.

Gestión y Revisión

El cifrado de sesiones mediante protocolos como TLS o IPSec no requiere protección adicional a nivel de hardware, salvo en escenarios donde un compromiso represente un riesgo catastrófico, como operaciones transaccionales en Inversiones Financieras. Sin embargo, los protocolos, algoritmos y módulos de cifrado se revisan anualmente, validando excepciones a la política de seguridad para mantener su efectividad frente a nuevas amenazas. Asimismo, los controles de seguridad aplicados al cifrado y protección de datos se evalúan cada año, identificando y corrigiendo posibles fallas operativas, un proceso que asegura la alineación con estándares internacionales y normativas sectoriales.

Impacto y Valor

Este enfoque estratégico en la protección y cifrado de datos fortalece la resiliencia del Grupo Empresarial frente a amenazas cibernéticas, protegiendo activos críticos y garantizando la confianza de clientes y socios. Al integrar tecnologías avanzadas como PQC y mecanismos de autenticación robustos, el programa no solo cumple con regulaciones estrictas, sino que también posiciona al grupo como un líder en ciberseguridad, capaz de ofrecer servicios de protección de datos a terceros, como aeropuertos o socios financieros, generando valor comercial en un mercado competitivo.

15. Clasificación de la Información

El Grupo Empresarial define los criterios y la metodología corporativa para el inventario, clasificación y etiquetado de sus activos de información, consolidándolos como un pilar estratégico en la gestión integral de activos, en estricta alineación con las políticas de ciberseguridad. Este enfoque asegura que la información reciba el nivel de protección adecuado según su valor y criticidad, fortaleciendo la seguridad en Manufactura, Energía, Concesiones e Inversiones Financieras, y cumpliendo con normativas como NERC CIP, GDPR, FAA e ISA99, mientras se protege contra riesgos emergentes en un entorno global.

Definición y Alcance de la Información Empresarial

La información empresarial comprende todos los datos de los que el Grupo Empresarial es titular o custodio, relacionados con su actividad mercantil. Esto incluye conocimientos, secretos empresariales, información estratégica, económica, tributaria, administrativa, operativa, y aquella protegida por propiedad intelectual o regímenes legales específicos. En 2025, el programa reconoce la importancia de proteger datos en un contexto de creciente interconexión y amenazas avanzadas, como accesos no autorizados a sistemas críticos o vulneraciones de datos personales, asegurando la confidencialidad, integridad y disponibilidad en todas las industrias del grupo.

Clasificación de la Información Empresarial

La información empresarial se clasifica según su nivel de acceso y uso, priorizando su protección. La información de acceso restringido incluye datos reservados, secretos empresariales, protegidos por propiedad intelectual, confidenciales, de procesos de contratación, organizacionales, con datos personales, y de terceros bajo custodia. Por ejemplo, la información reservada—como datos financieros o tributarios—solo puede ser consultada por accionistas y directivos autorizados, cumpliendo con el Código de Comercio, mientras que los secretos empresariales, como conocimientos estratégicos no patentables, requieren medidas de seguridad de alto nivel, incluyendo registros de acceso y modificaciones. La información protegida por propiedad intelectual, como signos distintivos o software desarrollado internamente, se restringe a usos empresariales autorizados, con el Área de Comunicaciones supervisando excepciones. La información confidencial abarca datos de clientes, proveedores, y proyectos estratégicos, mientras los datos personales se rigen por la Ley 1581 de 2012, asegurando su protección en todas las empresas del grupo.

Por otro lado, la información de acceso público se divide en pública interna, que puede compartirse entre áreas para fines operativos, y pública externa, como la misión, visión, valores corporativos, o datos inscritos en el registro mercantil, siempre bajo las restricciones definidas por el grupo. Los ciberactivos críticos, como aquellos que usan protocolos enrutables o son accesibles externamente, también se clasifican como restringidos, garantizando controles adicionales para proteger infraestructura crítica en Energía y Manufactura.

Inventario de Activos de Información

El inventario de activos de información es un proceso estructurado que identifica y documenta cada activo con características clave: nombre, descripción, propietario, área asociada, presencia de datos personales, contenedor (físico o electrónico), custodio, clasificación, y criticidad. Por ejemplo, un activo puede incluir bases de datos de clientes almacenadas en SharePoint o servidores externos, con un propietario definido que establece los controles necesarios. Si el activo contiene datos personales, se registra conforme a la Ley 1581 de 2012, detallando finalidad, titulares, y medidas de seguridad. Este inventario, revisado anualmente, asegura una gestión precisa y actualizada, protegiendo datos en todas las industrias del grupo.

Clasificación y Criticidad

La clasificación de activos se basa en los pilares de seguridad: confidencialidad, integridad y disponibilidad, alineados con estándares como ISO 27001. La confidencialidad se categoriza en niveles alta (reservada o secreta), media (confidencial), y baja (interna o pública), definiendo quién puede acceder a la información y bajo qué condiciones. La integridad evalúa el impacto de modificaciones no autorizadas, clasificando activos en alta, media o baja según las consecuencias operativas o económicas. La disponibilidad mide el tiempo aceptable de indisponibilidad, priorizando activos que, si no están accesibles en menos de un día, generan impactos significativos. La criticidad combina estos criterios, identificando activos de alta prioridad (por ejemplo, con confidencialidad alta) para asignarles controles más estrictos, asegurando la protección de datos estratégicos en Inversiones Financieras y Concesiones.

Etiquetado y Manipulación

El etiquetado de activos se basa en la confidencialidad, aplicando pautas rigurosas. La información reservada, secreta o confidencial requiere cifrado para su transmisión y almacenamiento, rótulos visibles (digitales o impresos), y almacenamiento seguro bajo llave, evitando accesos no autorizados. Para su destrucción, se emplean técnicas de borrado seguro, y los documentos impresos se transportan en sobres sellados. La nomenclatura de etiquetas sigue el formato ID-Confidencialidad-Disponibilidad-Integridad, facilitando su identificación, como “0001-MC-A-M” para un activo con confidencialidad media, integridad alta, y disponibilidad media. Este proceso asegura que los datos sensibles en todas las industrias estén protegidos y manejados adecuadamente.

Repositorios y Almacenamiento

El programa recomienda herramientas seguras para el almacenamiento de información. OneDrive se utiliza para datos internos o confidenciales que los empleados necesitan compartir, permitiendo colaboración segura.

Las herramientas de colaboración facilitan el intercambio de información pública o interna en reuniones, mientras SharePoint almacena datos confidenciales o secretos comunes a procesos, como contratos o indicadores. La información de criticidad alta, como actas de juntas directivas o bases de datos personales, se custodia en aplicaciones de negocio o sitios restringidos de SharePoint. El uso de discos duros portátiles está prohibido para documentos corporativos, minimizando riesgos de fuga de información.

Procedimiento de Gestión

El procedimiento para el inventario, clasificación y etiquetado consta de cuatro etapas. En la definición, un equipo responsable en cada compañía identifica los activos a inventariar, trabajando con los dueños de procesos para validarlos anualmente. La revisión verifica la relevancia de los activos y ajusta su clasificación ante cambios organizacionales, nuevos procesos, o migraciones de sistemas. La actualización incorpora estos cambios al inventario, y la publicación asegura que el documento sea clasificado como “Confidencial”, con acceso restringido a modificaciones, compartiendo la clasificación con custodios para aplicar los controles necesarios. Este procedimiento fortalece la gestión de datos en el grupo, asegurando su seguridad y cumplimiento normativo.

Impacto y Valor

Con la clasificación de la Información se busca una gestión segura de datos, protegiendo activos críticos y minimizando riesgos de divulgación no autorizada. Al implementar un enfoque estructurado, el programa de ciberseguridad garantiza el cumplimiento de normativas, fortalece la confianza de clientes y socios, y habilita oportunidades comerciales, como la oferta de servicios de gestión de datos a terceros, consolidando su ventaja competitiva.

16. Concientización en Ciberseguridad

La acelerada transformación digital impulsada por la pandemia ha expuesto a las organizaciones a nuevas amenazas cibernéticas, especialmente aquellas basadas en ingeniería social. Los atacantes ya no dependen exclusivamente de vulnerabilidades técnicas, sino que explotan los errores humanos mediante técnicas como el phishing, la manipulación o el engaño. En este contexto, los colaboradores y contratistas se convierten en el primer escudo de defensa. Por tanto, se hace esencial establecer una estrategia estructurada de cultura y concientización que eduque, sensibilice y empodere al personal frente a los riesgos digitales emergentes. Esta estrategia debe ir más allá de la simple formación, y buscar un cambio sostenido de comportamiento hacia una actitud consciente y preventiva. Véase: Programa de Cultura y Conciencia en Seguridad.

Propósito y Objetivo del Programa de Concientización

El programa de cultura y concientización tiene como propósito mejorar de manera tangible la postura de seguridad de la organización, priorizando la gestión del “riesgo humano”. Se busca desarrollar una conciencia colectiva que promueva el autocontrol en seguridad, la disciplina operativa y el compromiso de cada colaborador

con la protección de los activos digitales. Entre sus objetivos se incluyen la protección de la información ante amenazas internas y externas, la mejora de la capacidad de respuesta ante incidentes, el fortalecimiento de la resiliencia organizacional, y la generación de una red de sensores humanos que permita detectar y reportar incidentes antes de que escalen. Además, se busca establecer métricas claras que midan la efectividad del programa y asegurar el respaldo constante de los líderes de la organización.

Justificación e Importancia Estratégica

Los controles técnicos, aunque cruciales, no son suficientes frente a los vectores de ataque centrados en el comportamiento humano. Acciones cotidianas como abrir un correo sospechoso, usar dispositivos USB desconocidos o interactuar con enlaces en redes sociales representan brechas que pueden ser explotadas por los atacantes. La falta de adherencia a las políticas de seguridad por parte de los empleados representa un riesgo significativo. De ahí que la sensibilización y capacitación continua se posicionen como la mejor respuesta preventiva para cerrar esas brechas y fortalecer la defensa colectiva de la organización.

El programa aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas, datos o redes de la organización. Es responsabilidad del equipo de Seguridad de TI liderar la ejecución y sostenibilidad del programa, con apoyo de Talento Humano y líderes de proceso. Sus tareas incluyen la identificación de públicos objetivo, el diseño de contenidos, la planificación de campañas, la elección de medios de difusión, y la evaluación del impacto. Todo esto se ejecuta bajo una planificación anual que permite mantener la continuidad, adaptabilidad y efectividad del programa.

Audiencias y Segmentación

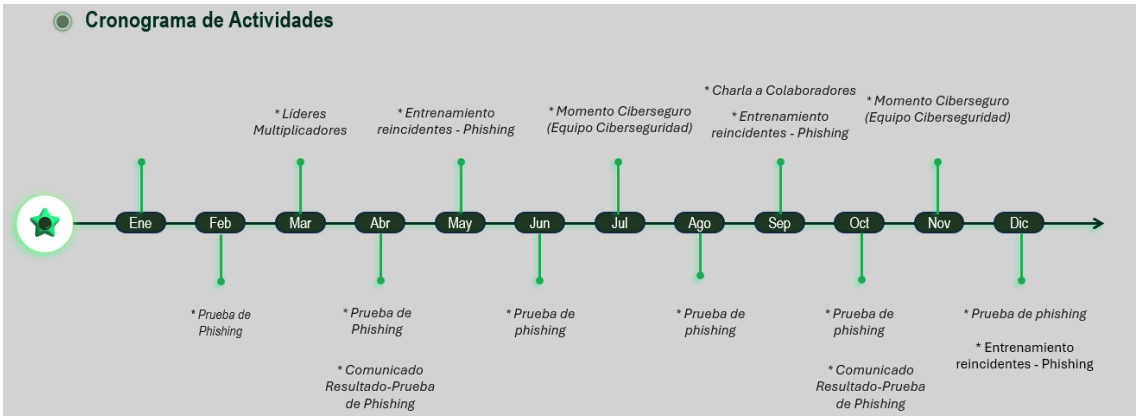
El programa reconoce que no todos los públicos requieren el mismo tipo de formación. Por ello, segmenta sus campañas en tres grandes grupos: el personal general (empleados y contratistas), los usuarios privilegiados (como administradores de sistemas), y los ejecutivos (como vicepresidentes o gerentes). Cada grupo recibe contenidos adaptados a su nivel de riesgo, tipo de acceso y rol estratégico dentro de la organización, mediante métodos como campañas visuales, capacitaciones dirigidas o plataformas de autoaprendizaje.

Riesgos Humanos que se buscan mitigar

Los riesgos humanos abordados por el programa incluyen la pérdida o divulgación de información, la alteración no autorizada de datos, la infección por malware, y errores humanos involuntarios como el envío incorrecto de información. El riesgo se define como la combinación entre la probabilidad de ocurrencia y el impacto del incidente, y puede originarse tanto por negligencia como por ataques deliberados. Las campañas buscan reducir estos riesgos a través de la concientización y la modificación de comportamientos inseguros.

Los temas abordados se seleccionan con base en su relevancia y aplicabilidad para todos los niveles de la organización. Incluyen el manejo de contraseñas, la detección de correos maliciosos, el uso seguro de redes

sociales, la protección de datos personales (Ley 1581), la respuesta a incidentes, y buenas prácticas durante viajes o trabajo remoto. También se incluyen temas técnicos específicos para usuarios privilegiados, como desarrollo seguro, seguridad en la nube y gestión de activos.

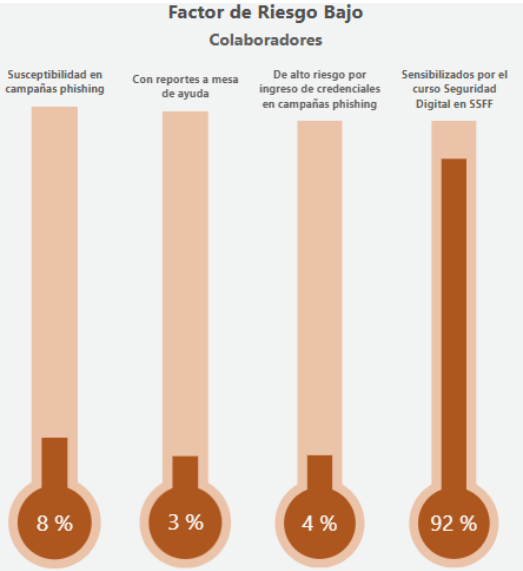


Técnicas de Comunicación y Canales de Difusión

Para garantizar una cobertura efectiva, el programa utiliza múltiples canales de comunicación: habladores físicos, intranet, correos electrónicos, fondos de pantalla, módulos e-learning, y redes sociales internas. Además, se refuerzan los mensajes clave mediante sesiones dirigidas y materiales visuales que buscan mantener la atención constante sobre los riesgos y buenas prácticas.

Evaluación, Métricas e Indicadores de Éxito

La efectividad del programa se mide a través de campañas simuladas de phishing, encuestas culturales, reportes de dispositivos perdidos y análisis del comportamiento ante amenazas. Las métricas se dividen en tres tipos: de cumplimiento (lo que se hace), de impacto (cambios de comportamiento) y estratégicas (reducción de incidentes). Estas permiten a los gestores tomar decisiones informadas, identificar áreas de mejora y reportar los avances a la alta dirección.



El programa se formaliza cada año en un plan detallado que incluye objetivos específicos, actividades por grupo objetivo, cronograma de campañas, técnicas de evaluación y acciones correctivas. Este documento guía la implementación continua y permite mantener un ciclo de mejora que garantice la madurez del programa a lo largo del tiempo.

El programa está alineado con estándares internacionales como ISO/IEC 27001 y SOC 2, cumpliendo con requisitos de formación exigidos para la gestión del sistema de seguridad de la información. Las capacitaciones obligatorias incluyen seguridad general, SGSI y desarrollo seguro, y su ejecución periódica respalda los controles de cumplimiento frente a auditorías y certificaciones.

17. Auditoria al programa de Ciberseguridad

La auditoría a la ciberseguridad constituye una función crítica dentro del modelo de gestión integral de riesgos tecnológicos y digitales. Su propósito es evaluar, de manera independiente y sistemática, la eficacia de los controles implementados, el nivel de madurez de los procesos, y el grado de cumplimiento con respecto a los marcos normativos, políticas internas y estándares internacionales. Además de permitir una evaluación retrospectiva, esta actividad actúa como un mecanismo de mejora continua, promueve la detección temprana de debilidades y fortalece la postura de defensa frente a amenazas emergentes. El proceso de auditoría no debe entenderse únicamente como una exigencia regulatoria o administrativa, sino como un habilitador estratégico para garantizar la resiliencia cibernética, la eficiencia operativa y la confianza digital de la organización.

El objetivo principal de este capítulo es establecer cómo las capacidades de ciberseguridad desplegadas en la organización son revisadas, validadas y fortalecidas mediante auditorías periódicas. Estas se realizan en estrecha coordinación con las áreas de auditoría interna y externa, asegurando su alineación con los riesgos

corporativos, las prioridades estratégicas y los marcos de gestión como NIST CSF, ISO/IEC 27001 y COBIT. Las auditorías permiten garantizar que los controles no solo existan en papel, sino que sean efectivos, medibles y estén correctamente integrados en los procesos de negocio.

Planes

Durante el año, se ha estructurado un plan de auditorías que abarca múltiples dimensiones del entorno digital y tecnológico. Estas auditorías han sido diseñadas con un enfoque basado en riesgos y cubren tanto aspectos técnicos como estratégicos. Entre los proyectos más relevantes se incluyen auditorías con Ethical Hacking sobre plataformas críticas, la revisión del nivel de ciberresiliencia organizacional con apoyo de consultores especializados, y la validación de iniciativas de transformación digital. También se han priorizado auditorías dirigidas a revisar la estrategia de ciberseguridad en su conjunto y los controles implementados en proveedores estratégicos, como parte de un enfoque más robusto hacia la gestión de riesgos en la cadena de suministro.

Alcance de las auditorías

El alcance de estas auditorías es amplio y abarca elementos esenciales de la ciberseguridad empresarial. En primer lugar, se analiza la gobernanza, es decir, la existencia y aplicación de políticas, planes estratégicos, roles definidos y mecanismos de supervisión adecuados. En segundo lugar, se evalúan aspectos técnicos, tales como la realización de pruebas de penetración (Ethical Hacking), revisiones de configuraciones, escaneos de vulnerabilidades y análisis de cumplimiento frente a benchmarks de seguridad reconocidos como los del CIS (Center for Internet Security). Otro componente esencial es la resiliencia organizacional, medida a través de la madurez de los planes de continuidad del negocio (BCP), recuperación ante desastres (DRP) y manejo de crisis (PMC), todos ellos evaluados no solo en su documentación, sino también en su aplicabilidad y pruebas prácticas. Asimismo, se revisan los controles aplicables a terceros y proveedores estratégicos, incorporando visitas in situ y análisis del cumplimiento contractual de cláusulas de seguridad. Finalmente, se considera la integración de la ciberseguridad en iniciativas de innovación y transformación digital, asegurando que los principios de "security by design" estén presentes desde las fases tempranas del ciclo de vida de los proyectos.

Integración con el Programa de Continuidad

Un aspecto fundamental de este enfoque de auditoría es su integración con el Programa de Continuidad del Negocio. Las revisiones permiten identificar sinergias y dependencias entre el procedimiento de atención de incidentes de ciberseguridad, los planes de continuidad operativa, los planes tecnológicos de recuperación ante desastres y los planes de manejo de crisis institucionales. Esta integración resulta crítica para garantizar que, ante un evento disruptivo —como un ciberataque, una pérdida masiva de datos o una afectación a la cadena de suministro digital—, la respuesta de la organización sea rápida, coordinada y efectiva. Las auditorías permiten verificar si los escenarios contemplados en los BCP y DRP incluyen incidentes cibernéticos, si se han realizado simulacros específicos para ataques tipo ransomware o exfiltración de información, y si existe una trazabilidad clara de las responsabilidades durante la gestión de crisis.

Como resultado de estos ejercicios, se generan recomendaciones y planes de mejora priorizados según su nivel de criticidad y el riesgo inherente que representan para la organización. Estos planes de acción incluyen

medidas correctivas y compensatorias, y son gestionados bajo herramientas GRC (Gobierno, Riesgo y Cumplimiento) con seguimiento estructurado por parte del Comité de Ciberseguridad. Además, los avances y hallazgos relevantes son presentados en los Comités de Riesgo y Auditoría, garantizando así la visibilidad y supervisión al más alto nivel. Entre los beneficios de este proceso se destacan la corrección oportuna de desviaciones técnicas o normativas, el fortalecimiento de controles clave, la mejora de la cobertura de protección frente a amenazas emergentes, y el incremento de la madurez en la gobernanza de activos digitales.

Finalmente, Las lecciones aprendidas se documentan y se transfieren a los equipos responsables, no solo para resolver los hallazgos inmediatos, sino también para prevenir su recurrencia. Esta práctica ha derivado en mejoras concretas como la actualización de políticas, la integración de hallazgos recurrentes en los planes de capacitación anual, la automatización del seguimiento a hallazgos críticos y la revisión periódica de la madurez de la organización con base en modelos como el NIST CSF Tiers o el CMMI.