Política de Ciberseguridad Gauss Control

Gauss Control, considera que la información y los sistemas asociados son activos críticos que deben ser protegidos para asegurar el correcto funcionamiento de la empresa. La Política de Ciberseguridad está orientada a gestionar eficazmente la seguridad de la información tratada por los sistemas informáticos, así como los activos que participan en sus procesos.

1. Prevención
    - 1.1. Gestión de Acceso
    - 1.2. Protección contra Ataques de Fuerza Bruta
    - 1.3. Seguridad de la Red
    - 1.4. Actualizaciones y Parches
    - 1.5. Política de uso de dispositivos personales
    - 1.6. Política de clasificación y manejo de información
    - 1.7. Seguridad física y ambiental
2. Detección
    - 2.1. Monitoreo Continuo
    - 2.2. Análisis de Comportamiento
    - 2.3. Escaneos de Seguridad y Auditorías
3. Resolución
    - 3.1. Plan de Respuesta a Incidentes
    - 3.2. Recuperación ante Desastres
    - 3.3. Colaboración con Autoridades y Expertos Externos
    - 3.4. Mejora Continua
    - 3.5. Capacitación y concienciación
    - 3.6. Gestión de vulnerabilidades
    - 3.7. Seguridad en la cadena de suministro
    - 3.8. Plan de comunicación de incidentes

Esta Política tiene como objetivo garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información y cumplir con las Leyes y Reglamentaciones vigentes en cada momento, manteniendo un equilibrio entre los niveles de riesgo y un uso eficiente de los recursos, con criterios de proporcionalidad.

Esta política de ciberseguridad es de aplicación a todos los empleados, directivos y administradores de todas las sociedades que integran la compañía, incluyendo aquellas sociedades participadas sobre las que tenga un control efectivo, dentro de los límites previstos en la normativa aplicable.

Para ello establecemos los siguientes principios:

- Garantiza que los Sistemas de Información y Telecomunicaciones de que dispone Gauss Control, posean el adecuado nivel de ciberseguridad y resiliencia.
- Sensibiliza a todos los empleados, contratistas y colaboradores acerca de los riesgos de ciberseguridad y garantiza que disponen de los conocimientos, habilidades, experiencia y capacidades tecnológicas necesarias para sustentar los objetivos de ciberseguridad del Grupo.
- Potencia las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las nuevas amenazas.
- Impulsa la existencia de mecanismos de ciberseguridad y resiliencia adecuados para los sistemas y operaciones gestionados por terceros que presten servicios a Gauss Control.
- Se dota de procedimientos y herramientas que permiten adaptarse con agilidad a las condiciones cambiantes del entorno tecnológico y a las nuevas amenazas.
- Colabora con los organismos y agencias gubernamentales relevantes para la mejora de la ciberseguridad de la compañía, el cumplimiento de la legislación vigente y contribuye a la mejora de la ciberseguridad en el ámbito internacional.

A continuación se proponen los controles requeridos para implementar, en distintas etapas y secciones de la compañía.

1. Prevención

Prevención hace referencia al conjunto de medidas proactivas para proteger los sistemas y la información ante posibles amenazas. Incluye controles como firewalls, antivirus, autenticación multifactor, encriptación, políticas de acceso y actualizaciones de seguridad, entre otros. Su objetivo es prevenir incidentes y evitar que los atacantes puedan explotar vulnerabilidades.

1.1. Gestión de Acceso

- Establecer políticas de control de acceso basadas en roles.
- Implementar autenticación multifactor para usuarios con acceso a la plataforma.
- Regular la revisión y revocación de privilegios de acceso según las funciones laborales.

1.2. Protección contra Ataques de Fuerza Bruta

- Limitar el número de intentos de inicio de sesión.
- Implementar medidas de bloqueo automático en caso de intentos fallidos.
- Monitorear y registrar los intentos de acceso no autorizados.

1.3. Seguridad de la Red

- Utilizar firewalls para controlar el tráfico de red.
- Encriptar la comunicación entre usuarios y la plataforma.
- Establecer zonas de confianza y restricciones de acceso basadas en direcciones IP.

1.4. Actualizaciones y Parches

- Mantener actualizados todos los sistemas y aplicaciones.
- Realizar pruebas de vulnerabilidad después de cada actualización.
- Establecer un proceso para aplicar parches críticos de seguridad de manera urgente.

1.5. Política de uso de dispositivos personales

- Exigir antivirus, cifrado de datos y bloqueo de pantalla en dispositivos personales.
- Prohibir jailbreak/rooting en dispositivos móviles.
- Definir requisitos para acceder a información corporativa.

1.6. Política de clasificación y manejo de información

- Establecer niveles de clasificación según la criticidad de la información.
- Definir lineamientos para el correcto manejo y almacenamiento de información.

1.7. Seguridad física y ambiental

- Implementar controles de acceso físico a áreas críticas.
- Considerar amenazas ambientales e implementar planes de continuidad.

2. Detección

Detección se enfoca en implementar mecanismos para identificar actividades maliciosas y anomalías en los sistemas y redes. Algunas de las herramientas utilizadas son sistemas de detección de intrusos (IDS), análisis de registros, monitoreo de tráfico de red, escaneos de vulnerabilidad, entre otros. Permite reconocer indicadores tempranos de compromiso.

2.1. Monitoreo Continuo

- Implementar herramientas de monitoreo de seguridad en tiempo real.
- Configurar alertas para detectar patrones de tráfico inusual.
- Realizar análisis de registros de forma regular para identificar posibles amenazas.

2.2. Análisis de Comportamiento

- Utilizar soluciones de análisis de comportamiento para detectar actividades anómalas.
- Establecer umbrales de comportamiento y alertas para posibles desviaciones.

2.3. Escaneos de Seguridad y Auditorías

- Realizar escaneos de seguridad periódicos en la plataforma.
- Llevar a cabo auditorías de seguridad para identificar posibles vulnerabilidades.
- Programar análisis de seguridad después de cambios significativos.

3. Resolución

La Resolución cubre los procesos para responder efectivamente ante incidentes de seguridad, contener el daño, recuperar los sistemas y aprender de lo sucedido. Incluye planes de respuesta a incidentes, continuidad del negocio, colaboración con autoridades, comunicación a los interesados, investigación forense, eliminación de vulnerabilidades y mejora continua de las defensas.

3.1. Plan de Respuesta a Incidentes

- Desarrollar y mantener un plan de respuesta a incidentes detallado.
- Definir roles y responsabilidades en caso de una amenaza a la disponibilidad.
- Realizar simulacros regulares para garantizar la efectividad del plan.

3.2. Recuperación ante Desastres

- Establecer procedimientos de respaldo y recuperación para minimizar el tiempo de inactividad.
- Almacenar copias de seguridad en ubicaciones seguras y accesibles.

3.3. Colaboración con Autoridades y Expertos Externos

- Colaborar con las autoridades pertinentes en caso de un incidente grave.
- Mantener contactos con expertos externos en ciberseguridad.

3.4. Mejora Continua

- Evaluar y revisar regularmente la eficacia de las medidas de seguridad.
- Actualizar la política y los procedimientos según las lecciones aprendidas.

3.5. Capacitación y concienciación

- Implementar campañas regulares para educar al personal sobre políticas y buenas prácticas de seguridad.
- Realizar simulacros de phishing y capacitaciones.

3.6. Gestión de vulnerabilidades

- Establecer procesos para identificar, priorizar y remediar vulnerabilidades de forma continua.
- Realizar evaluaciones de seguridad y ethical hacking de forma periódica.

3.7. Seguridad en la cadena de suministro

- Definir requisitos de seguridad para proveedores y socios.
- Evaluar riesgos de terceros y realizar auditorías regulares.

3.8. Plan de comunicación de incidentes

- Definir canales y responsables para reportar incidentes internamente.
- Establecer criterios para escalar y comunicar incidentes graves.

Esta política se revisará anualmente o en caso de cambios significativos en la infraestructura de la plataforma.

Fecha	Revisión	Historial del documento	Responsable
11-11-2023	1	Creación	Ana San Martín
16-11-2023	2	Incorpora conceptos de concientización y uso de equipos personales.	Andrés Gibson
16-11-2023	3	Publicación	Ana San Martín