Política de Seguridad de la Información

Versión 2.0 - BORRADOR

■ DOCUMENTO CONFIDENCIAL

Chief Information Security Officer (CISO)

1. Objetivo y Alcance

1. Objetivo y Alcance establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

1. Objetivo y Alcance establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

2. Marco Normativo ISO 27001

2. Marco Normativo ISO 27001 establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

2. Marco Normativo ISO 27001 establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

3. Clasificación de la Información

3. Clasificación de la Información establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

3. Clasificación de la Información establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

4. Control de Acceso

4. Control de Acceso establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

4. Control de Acceso establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

5. Gestión de Contraseñas

5. Gestión de Contraseñas establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

5. Gestión de Contraseñas establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

6. Seguridad en Redes

6. Seguridad en Redes establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

6. Seguridad en Redes establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

7. Protección de Datos Personales

7. Protección de Datos Personales establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

7. Protección de Datos Personales establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

8. Respuesta a Incidentes

8. Respuesta a Incidentes establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

8. Respuesta a Incidentes establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

9. Continuidad del Negocio

9. Continuidad del Negocio establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

9. Continuidad del Negocio establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

10. Cumplimiento y Auditoría

10. Cumplimiento y Auditoría establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.

10. Cumplimiento y Auditoría establece las directrices y controles necesarios para proteger los activos de información de la organización contra amenazas internas y externas. Esta política se basa en las mejores prácticas de la norma ISO/IEC 27001:2022 y aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información corporativos. Es responsabilidad de cada usuario cumplir con estas políticas y reportar cualquier incidente de seguridad de manera inmediata al área de TI. El incumplimiento de estas políticas puede resultar en acciones disciplinarias según el reglamento interno.