Política Seguridad de la Información

UC-United Capital Puesto de Bolsa, S.A.
Miembro de la Bolsa de Valores de la República Dominicana
SIV-PB-017

Contenido

Antecedentes

Nuestra organización procura: i) la seguridad de sus activos de información, ii) la ciberseguridad de las Tecnologías de Información y Comunicaciones (TIC) que soportan la infraestructura crítica del sector financiero y la operación de Puesto de Bolsa, y iii) la ciberseguridad de los activos tangibles e intangibles que son vulnerables a través de las TIC.

Para el cumplimiento de dicha misión se han adoptado mejores prácticas y ha propuesto la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), el cual está conformado por políticas, estándares (técnicos y generales de seguridad de la información), arquitectura computacional, procesos y procedimientos, estructura organizacional y mecanismos de verificación y control; y tiene como propósito garantizar que los riesgos de seguridad de la información y los riesgos de ciberseguridad sean conocidos, asumidos, gestionados y mitigados de forma documentada, sistemática, estructurada, repetible, eficiente y adaptable a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Las Políticas de Seguridad de la Información y Ciberseguridad son elementos fundamentales dentro del SGSI, puesto que contienen directrices que enmarcan la actuación de todos los empleados y contratistas de nuestra organización.

1. Objetivos

Las Políticas de Seguridad de la Información y Ciberseguridad tienen por objetivo la protección de los activos estratégicos de nuestra organización que dependen o usan las tecnologías de la información y las comunicaciones. Los objetivos específicos de esta política son:

- Establecer directrices generales relacionadas con seguridad de la información y ciberseguridad.
- Ser un medio de divulgación para comunicar los lineamientos establecidos por la Alta Gerencia de nuestra organización, respecto a la seguridad de la información y la ciberseguridad, generando cultura y compromiso en todos los niveles de la organización.
- Establecer y comunicar la responsabilidad y autoridad sobre el manejo de la seguridad de la información y la ciberseguridad de nuestra organización.
- Orientar el debido cuidado y la debida diligencia en la gestión de la seguridad de la información y la ciberseguridad.
- Establecer un orden y marco de actuación en temas de seguridad de la información y ciberseguridad, para todas las personas que presten sus servicios a United Capital.
- Garantizar la confiabilidad, imagen y credibilidad de Nuestra organización con sus empleados, clientes y relacionados.
- Definir un lenguaje común sobre la seguridad de la información y la ciberseguridad dentro de la organización.

2. Alcance

Esta política aplica a todos los empleados, consultores, contratistas y relacionados para manejo de la información propiedad de United Capital, abarcando todos los ámbitos de un SGSI.

3. Definiciones/Glosario

Para tales efectos se adoptan las siguientes definiciones:

- **Custodio:** Persona o el área responsable de proteger la información, de acuerdo con los lineamientos establecidos por el Generador (ver definición más adelante).

- **Estándar de Seguridad de la Información:** Conjunto de requisitos de obligatorio cumplimiento que especifica tecnologías, métodos y delimita las responsabilidades respecto de la seguridad de la información; así mismo establece pautas de acciones, según lo que les corresponda a las áreas en el ámbito de sus funciones.

- **Evidencia Digital:** Información con valor probatorio generada, transmitida o almacenada en forma digital (generada por computador o generada por medio diferente y almacenado o transmitido por computador).

- **Generador o Responsable:** Persona o área que crea la información.

- **Incidente de Seguridad de la Información:** Cualquier evento adverso que afecte o amenace los fundamentos de seguridad de la información (Confidencialidad, Integridad, Disponibilidad), de tal manera que genere un impacto negativo sobre la información de Nuestra organización.

- **Incidente de Ciberseguridad:** Es cualquier evento adverso, real o sospechoso, que afecte o amenace con afectar las TIC de Nuestra organización que soportan servicios críticos prestados al sistema financiero o la operación de Nuestra organización.

- **Información Corporativa:** Aquella que cumple con al menos una de las siguientes características:

    a) Se produce, envía o recibe en desarrollo de una función, actividad, servicio u operación, asignada a United Capital.

    b) Sirve de sustento o prueba de derechos, obligaciones o responsabilidades a cargo de nuestra organización o de terceros en relación con el mismo.

c) Aquella en la que constan las decisiones, normas o políticas tomadas o establecidas por las instancias competentes de Nuestra organización.

d) Se genera como resultado de la interacción entre nuestra organización y sus clientes, contratistas, o usuarios, que puede ser de interés para éstos o puede generar efectos jurídicos.

e) Se requiere con el fin de dar cumplimiento a alguna norma o política, dejar evidencia y prueba fehaciente de las actuaciones realizadas por los empleados de nuestra organización o por terceros que le prestan servicios.

f) Contribuye a la memoria institucional.

- **Personas que prestan servicios a United Capital**: Comprende directivos, empleados, contratistas, empleados temporales, pasantes y otros terceros que prestan servicios a United Capital.

- **Usuario:** Es aquella persona o área que ha sido autorizada por el Generador para tener acceso a cierta información.

- **Resiliencia:** Capacidad de continuar prestando servicios ante la materialización de eventos adversos críticos contra los activos de información y plataforma tecnológica.

- **Recursos de Tecnología de Información:** Recursos o apoyos tecnológicos ofrecidos por nuestra organización a los empleados para el normal desempeño de sus funciones (ej.: correo, Internet, teléfonos, computadores personales, servidores de archivo, cuentas de acceso, etc.).

- **Las Tecnologías de la Información y las Comunicaciones (TIC):** Son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes.

- **Infraestructura Crítica:** Activos y sistemas, físicos o virtuales, que son tan vitales para la organización que la obstrucción o destrucción de estos activos y sistemas, podría ocasionar impactos adversos en la ciberseguridad institucional, daño reputacional, perdida de integridad, confidencialidad y disponibilidad de la información o una combinación factores.

4. Política General de Seguridad de la Información

1. Nuestra organización cuenta con un Sistema de Gestión de la Seguridad de la Información (SGSI) que apoya una adecuada gestión de riesgos. Dicho Sistema soportará la debida protección de la información a partir de principios universalmente aceptados de seguridad de la información (Confidencialidad, Integridad, Disponibilidad).

2. Nuestra organización valora la información desde el punto de vista de seguridad y acorde a ello determina los mecanismos de protección adecuados.

3. Nuestra organización desde las etapas iniciales de los proyectos, incluye la evaluación de aspectos relacionados con la arquitectura de seguridad y sigue los lineamientos establecidos al respecto.

4. Nuestra organización atiende los incidentes relacionados con la seguridad de la información y ciberseguridad.

5. Nuestra organización implementa mecanismos para vigilar y promover el buen uso de los recursos tecnológicos.

6. Nuestra organización implementa mecanismos de concientización mediante un programa de formación y concientización continua a colaboradores de manera integral.

6. Nuestra organización implementa mecanismos para vigilar y promover el buen uso de la información.

7. Nuestra organización implementa controles de acceso (físicos y lógicos) para que la información corporativa se encuentre debidamente protegida. Así mismo, tiene mecanismos para seguimiento de actividades no autorizadas sobre la información o recursos de tecnología.

8. Nuestra organización implementa mecanismos y procedimientos para minimizar los riesgos asociados a la gestión de la información en los procesos que soportan la operación del negocio.

9. Nuestra organización implementa mecanismos y procedimientos para minimizar los riesgos asociados a la administración de la plataforma tecnológica que soporta la operación del negocio.

10. Nuestra organización implementa un programa de ciberseguridad alineado con mejores prácticas de seguridad y en cumplimiento al reglamento de Seguridad Cibernética y de la información emitido por la junta monetaria en enero 2018. Dicho programa busca el mejoramiento continuo de su postura de seguridad y aumentar su resiliencia

7. Control de versiones

La siguiente tabla muestra el historial de versiones de este documento:

Versión	Fecha	Preparado por	Razón de actualización
V 1.1	Junio 2019	Junior Ortiz Lahoz	Documento inicial
V 1.2	Octubre 2020	Junior Ortiz Lahoz	Actualizacion

8. Aprobaciones

Revisado por:	Gerente General	**Firma:**	
Aprobado por el Comité de Riesgo:	Presidente del Comité de Riesgo	**Firma:**	
	Vocal del Comité de Riesgo	**Firma:**	
	Secretario del Comité de Riesgo	**Firma:**	
Fecha Actualización	Octubre 2020		

Final del Documento.