Banesco Banco Universal 71

RIF: J-070133805

Caracas,____ de _____ de _____

Señores

_____

Presente.-

Atención: _____

REPRESENTANTE LEGAL

NORMATIVA DE SEGURIDAD PARA COMERCIO ELECTRÓNICO AFILIADOS A BANESCO BANCO UNIVERSAL

1.- Bloquear los USER ID de manera DEFINITIVA o TEMPORAL, que presentan códigos de rechazos con NIVEL DE RIESGO: **Muy Alto** o **Alto**, como se especifica en el anexo (**TABLA DE CÓDIGOS DE RECHAZOS SEGÚN EL NIVEL DE RIESGO**); puesto que este comportamiento es de riesgo. **Estos bloqueos de los USER ID de forma definitiva o temporal deben ser parametrizables.**

NOTA: los usuarios que sean bloqueados por algunos de estos códigos de rechazos, según su NIVEL DE RIESGO, deben ser deslogueados de la sesión automáticamente, mostrándoles los Mensajes o Banner, como se especifica en el anexo (**Mensaje o Banner por Nivel de Riesgo para Bloqueos de USER ID en Comercio Electrónico**).

2.- Con relación al proceso de afiliación y/o registro de los USER ID en la página del comercio electrónico, es implementar lo siguiente:

2.1.- Que en el proceso de afiliación se solicite al cliente (USER ID) la mayor cantidad de datos posibles, con los se puedan identificar patrones de riesgo o realizar análisis de estudio sobre los nuevos usuarios:

- User Id
- Cédula de Identidad. **Ver punto 2.2, 2.3 y 2.4**
- Nombre del Usuario. **Ver punto 2.2, 2.3 y 2.4**
- Cuenta de Correo Electrónico.
- N° de Teléfono de Habitación (Obligatorio).
- N° de Teléfono Móvil (Obligatorio).
- N° de Teléfono de Empresa (Opcional).
- Dirección de Habitación (Obligatorio).
- Dirección de Empresa (Opcional).
- Fecha de Nacimiento (Obligatorio).

NOTA: la "Dirección de Habitación" de ser solicitada de forma estructurada: Estado, Ciudad, Sector, Tipo de Vivienda, Calle o Avenida, Casa o Edificio.

2.2.- Es obligatorio que en el proceso de afiliación de los USER ID, se solicite el **N° de Cédula de Identidad; y luego, debe haber un procedimiento manual o automático,** que permita garantizar que el Nombre del Tarjetahabiente colocado en el proceso de afiliación sea verdadero.

2.3.- Es obligatorio, que el **N° de Cédula de Identidad** y el **Nombre del Tarjetahabiente previamente validado**, queden casados al USER ID; lo que significa, que éstos dos campos, NO deben ser modificados por los usuarios de la página web.

2.4.- Por lo tanto, al momento de la compra del producto o servicio, SOLO debe solicitarse: 1) **N° de Tarjeta de Tarjeta**, 2) **Fecha de Vencimiento** y 3) **Código de Seguridad**.

2.5.- **Se deben establecer montos límites por tarjeta: diario, mensual, anual. Estos límites por tarjeta deben ser por transacción y por acumulado (diarios, mensuales, anuales).**

2.6.- **Implementar Límite de uso de una misma tarjeta en el portal. La recomendación es que una tarjeta esté asociada a un solo USER ID. No deben haber dos o más USER ID utilizando la misma tarjeta. Una tarjeta por usuario.**

2.7.- **Un USER ID debe registrar un máximo de 1 o 2 tarjetas en el portal.**

3.- El Comercio Electrónico es responsable de crear una **LISTA NEGRA**, con los datos de los USER ID que han sido bloqueados de forma definitiva o temporal. Igualmente, crear una **LISTA NEGRA** con los datos de los USER ID que han presentado fraude, donde se actualicen automáticamente los datos fraudulentos registrados en la página web por los defraudadores; tales como:

3.1.- USER ID.
3.2.- Cuenta de Correo Electrónico.
3.3.- N° de Teléfono de Habitación.
3.3.- N° de Teléfono Móvil.
3.4.- Dirección de Habitación (Opcional)
3.5.- N° de Teléfono de Empresa
3.6.- Dirección IP

NOTA: de presentarse un nuevo USER ID que intente colocar alguno de los datos contenidos

en **LISTA NEGRA**, se debe rechazar la creación de este usuario, y se debe realizar una investigación con el fin de detectar nuevos patrones de fraude o posibles ataques de fraude a la página web.

4.- No está permitido que existan dos o más USER ID con el mismo N° de Cédula de Identidad y/o Correo Electrónico.

5.- Es obligatorio que al momento de la transacción, se implementen los siguientes mecanismos de control:

5.1.- Realizar una carga (micro pago) a la Tarjeta de Crédito por un monto mínimo aleatorio (inferior a 2,oo USD), previo a la compra del producto o prestación del servicio, a fin de autenticar al tarjetahabiente. El cliente debe verificar cuál es el monto con su banco, y que éste coincida con el monto que fue cargado de forma aleatoria. Luego debe ingresarlo en la página web del comercio electrónico para su validación.

NOTA: debe implementarse un **Bloqueo de usuarios en el portal si presentan más de 2 intentos de afiliación por micro pago fallido**.

5.2.- Es obligatorio que el campo **Código de Seguridad** sea solicitado a través de una función **CAPTCHA**, y no a través del teclado, a fin de evitar procesamiento o carga masiva de transacciones fraudulentas de tarjetas de crédito a través de un Robot.

6.- Restringir las direcciones IP de manera definitiva con recurrencia o reportes de fraude. Igualmente restringir las Dirección IP que estén presentado alto volumen de transacciones rechazadas con códigos de respuestas cuyo NIVEL DE RIESGO sea **Muy Alto** o **Alto**, como se especifica en el anexo (**TABLA DE CÓDIGOS DE RECHAZOS SEGÚN EL NIVEL DE RIESGO**).

7.- El Comercio Electrónico es responsable de crear un buzón de correo electrónico donde recibirá y enviará las alertas de posibles fraudes con tarjetas de crédito de las diferentes entidades.

8.- El Comercio Electrónico es responsable de realizar seguimiento a los casos de fraude que son reportados por los diferentes bancos emisores, a fin de Bloquear los USER ID, y los otros datos fraudulentos suministrados por los defraudadores, los cuales deben ser insertados en la **LISTA NEGRA**.

NOTA: Los datos de estos USER ID, deben ser incluidos en **LISTA NEGRA**, como se especifica en el punto N° 3.

9.- El Comercio Electrónico es RESPONSABLE de implementar un Sistema que detecte proactivamente los siguientes escenarios:

9.1.- Compras de productos o servicios desde diferentes Direcciones IP, realizadas con un mismo USER ID **en plazos de tiempos muy cortos**.

9.2.- Compras de productos por montos bajos, que al final no se concretan las entregas del pedido o la prestación del servicio. Se presume que los defraudadores realizan pruebas con las tarjetas, para luego realizar futuros fraudes.

9.3.- Uno o más USER ID que registren compras de productos o servicios **en plazos de tiempos muy cortos**, por montos elevados.

9.4.- Compras de boletos en diferentes salas de cine a nivel geográfico (distintas ciudades), realizada con un mismo USER ID en una misma fecha. **Esta recomendación solo aplica para el TIPO NEGOCIO: 7832 SALAS DE CINES Y TEATRO.**

10.- La cuenta corriente donde se depositan los cierres de las ventas, siempre debe contar con disponibilidad, a fin que Banesco Banco Universal pueda realizar los cargos (débitos) originados por los reclamos de consumos no reconocidos por fraude (Contracargos). De acuerdo a las cláusulas del Contrato de Pasarela de Pago y/o Teclado Abierto de Banesco Banco Universal.

11.- El personal que labora en la empresa _____, debe saber y dejarlo por escrito, que los datos sensibles de los Tarjetahabientes (**N° de Tarjeta de Crédito**, **Fecha de Vencimiento** y **Código de Seguridad**) no deben ser almacenados en ninguna base de datos o dispositivo de almacenamiento de información. Debe existir un acta firmada por cada empleado y dejar bien claras las consecuencias de incumplir con esta norma.

12.- Limitar el acceso de los operadores a las áreas de manejo de información sensible de medios de pagos de los clientes con dispositivos electrónicos y/o físicos como por ejemplo: papel, celular, cámaras, discos portátiles, entre otros.

13.- Acatar las normas de PCI para compras por comercio electrónico.

14.- Realizar Jornadas de Capacitación y Prevención para el personal que labora en las áreas administrativas, departamento de ventas, centro de atención al cliente, puesto que esto permitirá mitigar actividades inusuales que generen un riesgo a la empresa, o a los clientes de las diferentes entidades bancarias.

ANEXOS:

TABLA DE CÓDIGOS DE RECHAZOS SEGÚN EL NIVEL DE RIESGO

Código Respuesta Universal	Código Respuesta	Descripción Código de Respuesta	NIVEL DE RIESGO	BLOQUEO EN HORAS	INTENTOS	OBSERVACIONES	DIAS
000	00	APROBADO O COMPLETADO CON EXITO	N/A	N/A	N/A	N/A	N/A
001	01	LLAMAR AL EMISOR	Muy Alto	310	2	BLOQUEO TEMPORAL	15
003	03	COMERCIO NO VALIDO	Muy Alto	720	1	BLOQUEO TEMPORAL	30
004	04	RETENER TARJETA	Muy Alto	Definitivo	1	BLOQUEO DEFINITIVO	N/A
005	05	V- NO ACEPTAR/M- NO ACEPTAR	Muy Alto	720	1	BLOQUEO TEMPORAL	30
006	06	ERROR	Alto	360	2	BLOQUEO TEMPORAL	15
007	07	RETENER TARJETA (CONDICION ESPECIAL)	Muy Alto	Definitivo	1	BLOQUEO DEFINITIVO	N/A
008	08	ACEPTAR CON IDENTIFICACION	Alto	360	2	BLOQUEO TEMPORAL	15
009	09	CEDULA ERRADA	Muy Alto	720	2	BLOQUEO TEMPORAL	30
010	10	APROBADO POR MONTO PARCIAL	N/A	N/A	N/A	N/A	N/A
011	11	APROBADO (CLIENTE VIP)	N/A	N/A	N/A	N/A	N/A
012	12	TRANSACCION NO VALIDA	Muy Alto	720	2	BLOQUEO TEMPORAL	30
013	13	MONTO NO VALIDO	Muy Alto	720	2	BLOQUEO TEMPORAL	30
014	14	NUMERO DE TARJETA NO VALIDO	Muy Alto	720	2	BLOQUEO TEMPORAL	30
015	15	EMISOR NO VALIDO / COMERCIO BLOQUEADO	Muy Alto	720	2	BLOQUEO TEMPORAL	30
016	16	COMERCIO NO PERT.AL GRUPO CERRADO	Muy Alto	720	2	BLOQUEO TEMPORAL	30
017	17	CUPO FUERA DE FECHA	N/A	N/A	N/A	N/A	N/A
018	18	TRX NO PERMITIDA EN ESTE HORARIO	Alto	360	2	BLOQUEO TEMPORAL	15
019	19	TRX NO PERMITIDA ICSC ERRADO	Alto	360	2	BLOQUEO TEMPORAL	15
020	20	ARQC INVALIDO	Alto	360	2	BLOQUEO TEMPORAL	15
023	23	FALLBACK NO PERMITIDO	N/A	N/A	N/A	N/A	N/A
025	25	REGISTRO NO EXISTE	N/A	N/A	N/A	N/A	N/A
029	29	COD 19 VISA RE-ENTER TRANSACTION	Alto	360	2	BLOQUEO TEMPORAL	15
030	30	ERROR DE FORMATO	Alto	360	2	BLOQUEO TEMPORAL	15

031	31	ERROR FORMATO RETIRO DE EFECTIVO TAQUIL	N/A	N/A	N/A	N/A	N/A
039	39	TDC NO EXISTE	Muy Alto	720	2	BLOQUEO TEMPORAL	30
041	41	TARJETA EXTRAVIADA	Muy Alto	Definitivo	1	BLOQUEO DEFINITIVO	N/A
043	43	TARJETA ROBADA	Muy Alto	Definitivo	1	BLOQUEO DEFINITIVO	N/A
045	45	PIN PROVISIONAL ATM BANESCO	N/A	N/A	N/A	N/A	N/A
046	46	CAMBIO DE PIN NO EJECUTADO	N/A	N/A	N/A	N/A	N/A
047	47	PIN IGUAL A LOS ANTERIORES	N/A	N/A	N/A	N/A	N/A
051	51	FONDOS INSUFICIENTE/EXCEDE LIMITE CRED.	Medio	360	3	BLOQUEO TEMPORAL	15
054	54	VENCIMIENTO ERRADO	Alto	360	2	BLOQUEO TEMPORAL	15
055	55	PIN NO VALIDO	N/A	N/A	N/A	N/A	N/A
056	56	PIN PROVISIONAL ATM OTROS BANCOS	N/A	N/A	N/A	N/A	N/A
057	57	NO SE PERMITE LA TRANSACCION AL EMISOR	Muy Alto	720	2	BLOQUEO TEMPORAL	30
058	58	NOMBRE INVALIDO	N/A	N/A	N/A	N/A	N/A
059	59	TDC BLOQUEADA POSIBLE FRAUDE	Muy Alto	Definitivo	1	BLOQUEO DEFINITIVO	N/A
061	61	EXCEDE EL MONTO LIMITE DE RETIROS	N/A	N/A	N/A	N/A	N/A
062	62	TARJETA RESTRINGIDA	Muy Alto	Definitivo	1	BLOQUEO DEFINITIVO	N/A
063	63	VIOLACION DE SEGURIDAD	Muy Alto	Definitivo	1	BLOQUEO DEFINITIVO	N/A
065	65	EXCEDE EL CONTEO LIMITE DE RETIROS	N/A	N/A	N/A	N/A	N/A
069	69	BLOQUEO PREVENTIVO	Muy Alto	Definitivo	1	BLOQUEO DEFINITIVO	N/A
070	70	TARJETA CON SOBREGIRO	Alto	360	2	BLOQUEO TEMPORAL	15
071	71	TARJETA EN MORA	Alto	360	2	BLOQUEO TEMPORAL	15
072	72	EXCEDE PARAMETROS	Alto	360	2	BLOQUEO TEMPORAL	15
073	73	EXCEDE PARAMETROS	Alto	360	2	BLOQUEO TEMPORAL	15
074	74	EXCEDE PARAMETROS	Alto	360	2	BLOQUEO TEMPORAL	15
075	75	EXCEDIO EL NUMERO PERMITIDOS ENTRADA PI	N/A	N/A	N/A	N/A	N/A
076	76	LA CUENTA DE ENTRADA ESPECIF. NO VALIDA	N/A	N/A	N/A	N/A	N/A
077	77	LA CUENTA DE SALIDA ESPECIF. NO VALIDA	N/A	N/A	N/A	N/A	N/A
078	78	LA CUENTA ESPECIFICADA NO ES VALIDA	N/A	N/A	N/A	N/A	N/A
079	79	RESTRICCIÓN PAIS	Alto	360	2	BLOQUEO TEMPORAL	15
080	80	FECHA EFECTIVA INVALIDA(AMEX)	Alto	360	2	BLOQUEO TEMPORAL	15
081	81	4CSC INVALIDO (AMEX)	Muy Alto	720	2	BLOQUEO TEMPORAL	30
082	82	CVV NO VALIDO	Muy Alto	720	2	BLOQUEO TEMPORAL	30

083	83	CVC2/CVV2/3CSC INVALIDO	Muy Alto	720	2	BLOQUEO TEMPORAL	30
084	84	CICLO DE VIDA DE AUTORIZACION NO VALIDO	Alto	360	2	BLOQUEO TEMPORAL	15
085	85	NO DENEGADA	Alto	360	2	BLOQUEO TEMPORAL	15
086	86	MONEDA NO PERMITIDA (AMEX)	N/A	N/A	N/A	N/A	N/A
087	87	CONDICION CONTROL DE CAMBIO	N/A	N/A	N/A	N/A	N/A
088	88	COMERCIO NO AFILIADO A TT	N/A	N/A	N/A	N/A	N/A
089	89	ESTABLECIMIENTO CANCELADO AMEX	N/A	N/A	N/A	N/A	N/A
090	90	CAM FALLIDO CON VISA	Alto	360	2	BLOQUEO TEMPORAL	15
091	91	SISTEMA DEL EMISOR INOPERATIVO	Alto	360	2	BLOQUEO TEMPORAL	15
092	92	NO SE PUEDE ENVIAR LA TRANSACCION	Alto	360	2	BLOQUEO TEMPORAL	15
093	93	TX CANNOT BE COMPLETED, VIOLATION OF LA	Alto	360	2	BLOQUEO TEMPORAL	15
094	94	SE DETECTO UNA TRANSMISION DUPLICADA	Alto	360	2	BLOQUEO TEMPORAL	15
095	95	EXCEDE MONTO POR ESCALA	Alto	360	2	BLOQUEO TEMPORAL	15
096	96	ERROR DEL SISTEMA	Alto	360	2	BLOQUEO TEMPORAL	15
097	97	TX YA REVERSADA	N/A	N/A	N/A	N/A	N/A
098	98	EXCEDE DISP. AVANCE	N/A	N/A	N/A	N/A	N/A

Mensaje o Banner por Nivel de Riesgo para Bloqueos de USER ID en Comercio Electrónico

Nivel de Riesgo	Mensaje o Banner
Muy Alto	Le informamos que por medidas de seguridad nos vemos en la necesidad de suspender temporalmente su acceso al portal hasta validar sus datos. Si Usted tiene alguna observación, comuníquese inmediatamente con nosotros a través del número 0212- o correo electrónico, y gustosamente le atenderemos. Atentamente,

Alto	Estimado Cliente: Nuestro sistema nos reporta una alerta de uso indebido en su cuenta, motivo por el cual y por su seguridad, nos vemos en la necesidad de suspender temporalmente su acceso al portal hasta validar sus datos. Si Ud. tiene alguna observación o reclamo, comuníquese inmediatamente con nosotros al 0212- o correo electrónico, y gustosamente le atenderemos. Atentamente,
Medio	Le informamos que por medidas de seguridad nos vemos en la necesidad de suspender temporalmente su acceso al portal hasta validar sus datos. Si Usted tiene alguna observación, comuníquese inmediatamente con nosotros a través del número 0212- o correo electrónico, y gustosamente le atenderemos. Atentamente,
Bajo	Le informamos que por medidas de seguridad nos vemos en la necesidad de suspender temporalmente su acceso al portal hasta validar sus datos. Si Usted tiene alguna observación, comuníquese inmediatamente con nosotros a través del número 0212- o correo electrónico, y gustosamente le atenderemos. Atentamente,
Bloqueo Definitivo	Le informamos que por medidas de seguridad nos vemos en la necesidad de suspender Definitivamente su acceso al portal Atentamente,

Atentamente,

Gcia de Innovación y Tendencias / Gcia Req. Monitoreo de Fraude y Delitos Financieros

Banesco Banco Universal C.A.

Recibí Conforme.,

_____ _____ Nombre del Representante Legal Firma